La sécurité des traitements de données, les analyses d'impact et les violations de données

Dumortier, Franck

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 4
La sécurité des traitement de données, les analyses d'impact et les violations de données

Franck DUMORTIER[1]

Introduction

1. Dans le contexte actuel des tendances au BYOD[2], de l'IoT[3], du Cloud Computing[4], et plus généralement de l'interconnexion ascendante des systèmes, l'effectivité des droits fondamentaux à la vie privée et à la protection des données à caractère personnel dépend considérablement des mesures mises en place pour assurer la sécurité de celles-ci[5]. Ce lien de dépendance a notamment été illustré par la Cour européenne des droits

[1] Franck Dumortier est chercheur et maître de conférences au CRIDS. Il est chargé de cours en aspects légaux de la sécurité informatique dans le cadre du Master en cybersécurité. L'auteur est par ailleurs actuellement subsidié par le projet H2020 PROTECT (Pervasive and user focused biometrics borders project). *This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700259.*

[2] Le BYOD est une pratique consistant à autoriser les employés à utiliser, dans un contexte professionnel, leurs propres terminaux personnels. Les smartphones en sont l'exemple le plus commun, mais le BYOD peut également recouvrir les tablettes, les ordinateurs portables, ou encore les clés USB. Groupe 29, Avis 2/2017 sur le traitement des données sur le lieu de travail, WP 249, 8 juin 2017, p. 16.

[3] L'Internet des objets (en anglais « *Internet of Things* » ou IoT) représente l'extension d'Internet à des choses et à des lieux du monde physique. Groupe 29, Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, WP 223, 16 septembre 2014, p. 4.

[4] L'informatique en nuage (en anglais « *Cloud Computing* ») réunit un ensemble de technologies et de modèles de services dans lesquels l'utilisation et la livraison d'applications informatiques, la capacité de traitement, le stockage et l'espace mémoire reposent tous sur l'internet. Groupe 29, Avis 05/2012 sur l'informatique en nuage, WP 196, 1er juillet 2012, p. 4.

[5] Les articles 8 de la CEDH et 22 de la Constitution belge consacrent le droit au respect de la vie privée. Avec l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Charte des droits fondamentaux de l'Union européenne a acquis force juridique obligatoire et le droit à la protection des données à caractère personnel a été érigé au rang de droit fondamental autonome en son article 8 (en sus du droit à la vie privée consacré en son article 7).

de l'homme dans l'affaire *I. c. Finlande*[6] ; celle-ci estimant que le défaut de garanties relatives à la sécurisation des données contre des usages non-autorisés constitue une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'article 8 de la Convention européenne des Droits de l'homme (ci-après « CEDH »). Cette perception des choses est importante pour éclairer et interpréter l'obligation de sécurisation de données concernant des personnes physiques qui peuvent être identifiées directement ou indirectement[7]. Plus largement, la sécurité des « données informatiques »[8] est devenue un enjeu majeur pour notre vie sociale, notre économie, notre santé, voire notre intégrité physique – et par conséquent notre vie privée[9] –, qui dépendent désormais considérablement de technologies fonctionnant sans *discontinuité*. C'est la raison pour laquelle l'Union Européenne considère la « cyber-résilience » comme un objectif prioritaire[10], que fut adoptée la directive NIS[11] et que

[6] Cour eur. D.H., 17 juillet 2008, *I. c. Finlande*, req. n° 20511/03. Dans cette affaire, la requérante infirmière dénonce la consultation illégale de son dossier médical confidentiel par ses collègues de travail. Dans son arrêt, la Cour conclut, à l'unanimité, qu'il y a eu violation de l'article 8, les autorités internes n'ayant pas, au moment des faits, mis les données médicales de la requérante à l'abri d'un accès non autorisé.

[7] Cour eur. D.H., 4 décembre 2008, *Marper c. Royaume-Uni*, req. n^{os} 30562/04 et 30566/04, § 103. Selon la Cour, « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. […] Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voir notamment l'article 7 de la Convention [n° 108] sur la protection des données) ».

[8] Une définition de cette notion apparaît, par exemple, dans l'article 1er de la Convention de Budapest (Convention sur la cybercriminalité STE n° 185 du Conseil de l'Europe, Budapest, 11, 2001) qui définit « données informatiques » comme toute « représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ». Voy. égal., l'article 2, b), de la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

[9] La signification des quatre concepts protégés par l'article 8, § 1, de la CEDH n'est pas parfaitement explicite et la Cour évite de définir des règles précises concernant leur interprétation. En particulier, son approche consiste à évaluer l'applicabilité de l'article 8 et donc si une requête individuelle tombe dans le champ d'un des droits protégés au cas par cas, tout en conférant aux concepts une signification autonome au niveau de la Convention.

[10] Communication conjointe au Parlement européen, au Conseil, au comité économique et social européen et au comité des régions Stratégie de cybersécurité de l'Union européenne, « un cyberespace ouvert, sûr et sécurisé », adoptée le 7 février 2013.

[11] Directive 2016/1148/UE du Parlement européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après « directive NIS »).

l'obligation d'assurer, selon les besoins, « la disponibilité et la résilience constantes des systèmes et des services de traitement »[12] fut inscrite dans le règlement général sur la protection des données[13] (ci-après « RGPD »), lequel renforce sensiblement l'obligation de sécurité des données à caractère personnel telles qu'interprétées au sens large[14].

2. Sous l'empire de la Directive, les brèches de sécurité ne devaient pas explicitement être divulguées[15]. En 2014, le Groupe 29 rappela toutefois que l'obligation de sécurité imposée par l'article 17 de directive 95/46/CE[16] (ci-après « la Directive ») impose une gestion proactive des risques dans laquelle l'utilisation de mécanismes d'inintelligibilité (par exemple le chiffrement) des données est particulièrement recommandée afin de minimiser l'impact de fuites de données, lesquelles devraient, le cas échéant, être communiquées aux personnes concernées[17]. La même année, le Groupe 29 réaffirma que *l'approche fondée sur le risque* (« *risk-based approach* ») était au cœur du cadre légal régissant la protection des données[18], sans remettre pour autant en question les principes de protection des données ou les droits des personnes concernées.

---

[12] Art. 32, § 1, b), du RGPD.

[13] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[14] Voy. la définition large de « données à caractère personnel » prônée par le Groupe 29 dans son *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136, 20 juin 2007. Lire égal. Y. Poullet, « La protection des données : un nouveau droit constitutionnel - pour une troisième génération de réglementations de protection des données », in *Droit constitutionnel et vie privée*, Thunis, 2008 pp. 297-365. De manière analogue, selon notre approche, le concept de « donnée à caractère personnel » doit être compris au sens large, y compris en ce qui concerne les données de trafic telles des adresses IP ou MAC. À cet égard, lire C.J.U.E., 19 octobre 2016, arrêt *Patrick Breyer c. Bundesrepublik Deutschland*, C-582/14, § 49. Cette approche a d'ailleurs été rappelée par le Groupe 29 selon lequel « il y a lieu de noter que les adresses MAC sont des données à caractère personnel, y compris après la mise en œuvre de mesures de sécurité telles que le hachage ». Groupe 29, *Avis 01/2017 sur la proposition de règlement relatif au respect de la vie privée dans les communications électroniques (2002/58/CE)*, WP 247, 4 avril 2017, p. 13.

[15] À l'exception du secteur « télécom » dans lequel la directive 2002/58/CE sur la protection de la vie privée dans les communications électroniques a été amendée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 en vue notamment d'y introduire une disposition spécifique aux « violation de données à caractère personnel ».

[16] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281/31 du 23 novembre 1995.

[17] Groupe 29, Avis 03/2014 sur la notification des violations de données à caractère personnel, WP 213, 25 mars 2014, p. 3.

[18] Groupe 29, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, 30 mai 2014, p. 2.

C'est donc tout naturellement que le RGPD innove par rapport à la Directive en consacrant le principe « d'intégrité et de confidentialité » comme l'une des pierres angulaires de leur protection. L'élévation de l'obligation de sécurité au rang de principe de base n'est pas que théorique puisqu'elle soutenue dans le texte du règlement par l'impératif documentaire découlant du devoir d'*accountability*[19] ayant pour outils principaux l'établissement d'un registre des activités de traitements (ci-après « Registre »)[20] et, dans certains cas, la conduite d'une analyse d'impact (ci-après « AIPD »)[21]. La culture de la sécurité des données se voit également promue par l'introduction de mesures concrètes telle la protection des données dès la conception et par défaut[22] ainsi que par la possibilité de recourir à des codes de conduite ou des mécanismes de certification pour « faciliter » la démonstration du respect des exigences légales. De plus, dans la plupart des cas, les violations de données doivent maintenant être notifiées à l'Autorité de contrôle compétente (ci-après « APD ») et parfois même être communiquées aux personnes concernées[23]. Enfin, les manquements à l'obligation de sécurité sont dorénavant potentiellement punissables d'amendes administratives[24].

[19] Art. 5, § 2, et 24 du RGPD. Selon le Groupe 29, « [e]n français, le texte du RGPD utilise le terme « responsabilité ». En anglais, on utilise le terme « *accountability* », issu du monde anglo-saxon où il est d'usage courant et où il existe un vaste consensus sur le sens à lui donner – bien qu'il soit difficile d'en définir avec précision le sens dans la pratique. Globalement, on peut toutefois dire qu'il met l'accent sur la manière dont la responsabilité (*responsability*) est assumée et sur la manière de le vérifier. En anglais, les termes « *responsibility* » et « *accountability* » sont comme l'avers et le revers d'une médaille et sont tous deux des éléments essentiels de la bonne gouvernance. On ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (*responsability*) est efficacement assumée dans la pratique. Dans la plupart des autres langues européennes, du fait, essentiellement, de la diversité des systèmes juridiques, il est difficile de traduire le terme « *accountability* ». Groupe 29, Avis n° 3/2010 sur le principe de la responsabilité, WP 173, 13 juillet 2010, p. 8.

[20] Art. 30 du RGPD.

[21] Art. 35 du RGPD.

[22] Art. 25 du RGPD.

[23] Art. 34 du RGPD.

[24] Art. 83, § 4, a), et 83, § 5, a), du RGPD.

CHAPITRE 1. L'avènement d'un « nouveau » principe de base d'intégrité et de confidentialité

3. Une innovation remarquable du règlement est qu'il érige le principe « d'intégrité et de confidentialité » des données à caractère

personnel au même rang que les traditionnels principes de qualité des données (licéité, loyauté, transparence, finalité, minimisation, exactitude et limitation de la conservation des données). Il s'agit là d'une véritable reconnaissance du poids de la sécurité des données par le législateur puisque celle-ci n'était auparavant pas élevée au grade de principe dans la Directive. Toutefois, sous ce régime antérieur, on considérait déjà la sécurité des données à caractère personnel comme une condition *sine qua non* du respect de leurs principales dispositions[25]. Ainsi, Y. Poullet s'interrogeait en ces mots : « Sans elle, comment convaincre la personne concernée qui se prévaut de son droit d'accès, que les informations communiquées en conséquence de l'exercice de ce droit soient les seules détenues. Comment affirmer qu'aucune personne non autorisée n'aura jamais accès à des données détenues par le responsable pour des finalités illégitimes ? Comment enfin, garantir la personne concernée contre la non déformation des données voire l'ajout de certaines données non pertinentes ? »[26].

Qui plus est, depuis 1981, la sécurité des données fait déjà partie des « principes de base » énumérés par la Convention n° 108[27] du Conseil de l'Europe (ci-après « CoE »). L'Union européenne et la Belgique sont Parties de cette Convention et se sont engagées à prendre les mesures nécessaires pour donner suite à ce « noyau dur » dans leurs législations respectives. Ladite Convention a du reste fait l'objet d'une modernisation[28] et contient dans son texte révisé[29] un article 7 comprenant une règle portant sur les « violations des données » confortant l'idée que la sécurité des données ne peut se concevoir sans mécanisme de *reporting transparent* des incidents. Le fait que le RGPD ait regroupé les articles 32 (sécurité du traitement), 33 (notification d'une violation de données à l'APD) et 34 (communication à la personne concernée d'une violation de données) dans la même

[25] Y. Poullet, « La sécurité informatique, entre technique et droit », *Cahiers du CRID*, n° 14, 1998, p. 17.

[26] *Ibid.*

[27] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Référence, STE n° 108, 28 janvier 1981. Selon l'article 7 de celle-ci, « des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés ».

[28] À ce sujet, lire C. de Terwangne, « La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », in *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 81-120.

[29] Convention 108 modernisée, adoptée le 18 mai 2018, disponible à l'adresse https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4b.

section 2 (du Chapitre IV) du RGPD intitulée « sécurité des données à caractère personnel » n'est donc pas un hasard. Dans ce contexte, il est également intéressant de relever que le rapport explicatif de la « nouvelle » Convention n° 108 considère explicitement qu'une « notification à d'autres autorités compétentes, par exemple celles chargées de la sécurité des systèmes informatiques, peut également être souhaitable »[30]. Cette recommandation corrobore l'approche des articles 14 et 16 de la directive NIS qui imposent aux « opérateurs de services essentiels »[31] (ci-après « OSE ») ainsi qu'aux « fournisseurs de services numériques »[32] (Digital service providers, ci-après « DSP ») de notifier sans retard injustifié des *incidents ayant un impact significatif sur* la *continuité* de leurs services[33] et au(x) CSIRT(s) national/nationaux[34]. Certes, la notification des « incidents »[35] dans le contexte de la directive NIS poursuit un objectif différent de celui que s'est fixé le RGPD. Néanmoins, dans de nombreux cas, des données à caractère personnel[36] seront traitées à la suite d'incidents au sens de la Directive susmentionnée : « dans de telles circonstances, les autorités

[30] Conseil de l'Europe, Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 mai 2018, pt 66.

[31] Voy. l'article 4, 1), de la directive NIS selon lequel un OSE est défini comme : a) une entité publique ou privée qui fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ; b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; c) un incident aurait un effet disruptif important sur la fourniture dudit service. Pour le 9 novembre 2018 au plus tard, les États membres ont l'obligation d'identifier les OSE ayant un établissement sur leur territoire pour chaque secteur et sous-secteur visé à l'annexe II de la directive NIS (énergie, transports, banques, infrastructures de marchés financiers, secteur de la santé, fourniture et distribution d'eau potable, infrastructures numériques).

[32] Les types de fournisseurs de services numériques sont repris à l'annexe III de la directive NIS. Sont ainsi visés les « places de marché en ligne », les « moteurs de recherche en ligne » et « les services d'informatique en nuage » ayant leur établissement principal (siège social) ou un représentant désigné sur le territoire d'un État membre. En effet, un DSP qui n'est pas établi dans l'Union mais qui fournit des services susmentionnés à l'intérieur de l'Union doit désigner un représentant dans l'un des États membres dans lesquels les services sont fournis.

[33] Voy. l'article 8, § 3, de la directive NIS selon lequel chaque État membre doit désigner un point de contact national unique en matière de sécurité des réseaux et des systèmes.

[34] Un CSIRT est un centre de réponse aux incidents de sécurité informatique – également connu sous la dénomination de centre de réponse aux urgences informatiques (CERT) – chargé de la gestion des incidents et des risques selon un processus bien défini. En vertu de l'article 9 de la directive NIS, chaque État membre doit désigner un ou plusieurs CSIRT, se conformant aux exigences énumérées à l'annexe I, point 1) de ladite directive.

[35] Dans le contexte de la directive NIS, un « incident » est défini comme étant « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information », même en l'absence de traitements de données à caractère personnel.

[36] Au sens large : pensons, par exemple, aux adresses IP ou MAC.

compétentes [en matière de cybersécurité] et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents »[37]. Enfin, à l'instar de l'article 10 de la Convention n° 108 modifiée, le RGPD impose des devoirs complémentaires consistant, d'une part, à « procéder, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées »[38] et, d'autre part, d' « être en mesure de démontrer en particulier à l'autorité de contrôle compétente [...] que le traitement [...] est en conformité avec les dispositions de la Convention »[39].

[37] Considérant n° 63 de la directive NIS.
[38] Art. 10, § 2, de la Convention n° 108 modernisée.
[39] Art. 10 § 1er, de la Convention n° 108 modernisée.

CHAPITRE 2. Le principe d'intégrité et de confidentialité

SECTION 1. – Objet du principe

4. Conformément à l'approche du CoE, l'article 5, § 1, f), du RGPD élève le principe de sécurité des traitements au même rang que les classiques principes de qualité des données. Selon ce « nouveau » principe, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée, « *y compris* la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées »[40].

Toutefois, le principe énoncé dans le règlement peut sembler avoir un objet plus restreint que celui consacré dans la Convention n° 108 dans la mesure où la seconde protège la « sécurité des données »[41] au sens large alors que le premier se borne explicitement à garantir « l'intégrité et la confidentialité » de celles-ci. Cette limitation du principe de sécurité aux deux propriétés susmentionnées contraste également avec l'affirmation de l'ENISA selon laquelle « *one of the core obligations for data controllers and processors in GDPR is that of the security of personal data. In*

[40] Art. 5, § 1, f), du RGPD. Les termes « y compris » ne sont pas anodins puisqu'ils ne sont pas inscrits dans l'article 17, § 1, de la Directive.

[41] Art. 7 de la Convention n° 108.

particular, according to GDPR security equally covers confidentiality, integrity and availability »[42].

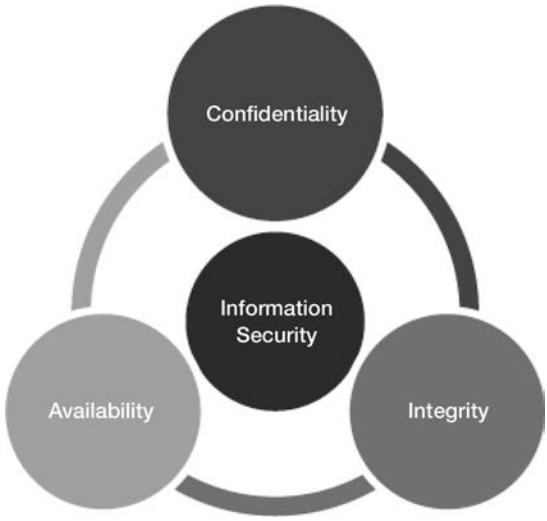

Figure 1 – La triade intégrité-confidentialité-disponibilité selon l'ENISA[43]

Pour rappel, l'ENISA est l'Agence Européenne chargée de la sécurité des réseaux et de l'information, telle que régie par le règlement (UE) 526/2013[44]. Dans sa proposition de refonte des objectifs et des tâches de ladite agence, la Commission rappelle l'importance de la cybersécurité dans les termes suivants : « *Cybersecurity has an essential role in protecting the privacy and personal data of individuals in accordance with Articles 7 and 8 of the Charter of Fundamental Rights of the EU. In case of cyber incidents the privacy and the protection of our personal data are clearly exposed. Cybersecurity is thus a necessary condition for the respect of privacy and confidentiality of our personal data. Under this perspective, by aiming to reinforce cybersecurity in Europe, the proposal provides an important complement to the existing legislation protecting the fundamental right to privacy and personal data. Cybersecurity is also essential for protecting the confidentiality of our electronic communications*

[42] ENISA, *Guidelines for SMEs on the security of personal data processing*, décembre 2016, p. 7.

[43] *Ibid*, p. 10.

[44] Règlement (UE) 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) 460/2004.

and thus for exercising the freedom of expression and information and other related rights, such as the freedom of thought, conscience and religion »[45].

Par conséquent, l'objet du principe édicté par l'article 5, § 1, f), du RGPD doit être lu dans un contexte européen plus large qui considère la cybersécurité[46] comme un enjeu crucial en vue d'assurer non seulement l'intégrité et la confidentialité[47] des données mais également la disponibilité et la résilience de *certains* systèmes et réseaux informatiques[48].

§ 1. L'intégrité et la confidentialité des données

5. Malgré un certain silence du RGPD sur la définition de la notion d'intégrité des données, le Groupe 29 considère que celle-ci peut se définir comme « la qualité en vertu de laquelle les données sont authentiques et n'ont pas été modifiées par mégarde ou malveillance pendant le traitement, le stockage ou la transmission. La notion d'intégrité peut s'étendre aux systèmes informatiques et exige que le traitement des données à caractère personnel sur ces systèmes reste inaltéré »[49].

Quant à la notion de confidentialité, le considérant n° 39 du RGPD suggère qu'elle consiste à « prévenir l'accès non autorisé à ces données et à

---

[45] *Proposal for a Regulation of the European Parliament and of the Council on ENISA the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')*, COM (2017) 477 final, 13 septembre 2017, p. 19.

[46] Selon l'article 2, 1), de la proposition de règlement susmentionnée « *cybersecurity comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats* ».

[47] Dans son WP 168, le Groupe 29 mentionne que « la Cour constitutionnelle allemande (arrêt du 27 février 2008 - 1 BvR 370/07 ; 1 BvR 595/07) a créé un droit constitutionnel à la confidentialité et à l'intégrité des systèmes informatiques. Les systèmes capables de créer, de traiter ou de stocker des données sensibles à caractère personnel requièrent une protection particulière. Le champ de protection du droit fondamental à la confidentialité et à l'intégrité des systèmes d'informations s'étend aux systèmes qui, seuls ou du fait de leur interconnectivité technique, peuvent contenir des données à caractère personnel sur la personne concernée, à un degré et dans une diversité tels que l'accès aux systèmes fournit des informations sur des éléments importants de la vie de cette personne ou dresse un portrait révélateur de sa personnalité. Ces systèmes sont par exemple les ordinateurs personnels et les ordinateurs portables, les téléphones portables et les agendas électroniques ». Groupe 29, L'avenir de la protection de la vie privée, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, WP 168, 1er décembre 2009, p. 15.

[48] En ce sens, voy. la communication conjointe au Parlement européen et au Conseil « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide », JOIN(2017) 450 final, 13 septembre 2017.

[49] Groupe 29, WP 196, *op. cit.*, p. 18.

l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement ». De plus, l'article 29 du RGPD stipule expressément que « le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre ».

Dans la même ligne, l'ENISA et la Commission de la vie privée belge[50] (« CPVP ») définissent l'intégrité d'une donnée comme étant « la propriété de ne pas être altérée *ou détruite* de manière non autorisée, volontairement ou accidentellement » et la confidentialité, celle « de ne pouvoir être accédée que par des personnes, entités ou processus autorisés et de ne pouvoir être divulguée qu'à des personnes, entités ou processus autorisés »[51]. Le Groupe 29 considère quant à lui que l'expression « violation de l'intégrité » correspond à l'altération non-autorisée ou accidentelle de données à caractère personnel et que les termes « violation de la confidentialité » couvrent l'accès non autorisé à celles-ci ainsi que leur divulgation inappropriée[52].

§ 2. Quid de la disponibilité des données ?

6. Les concepts d'intégrité et de confidentialité des données étant relativement clairs, le vocabulaire utilisé par le règlement pose néanmoins fondamentalement la question du sort réservé à la garantie de la *disponibilité des données*, non explicitement prévue par l'article 5, § 1, f), de celui-ci.

Ce questionnement est loin d'être théorique puisque dans le domaine de la sécurité de l'information[53] – lequel couvre un contexte sensiblement plus large que celui de la sécurité des données à caractère personnel –,

[50] Qui devient avec l'entrée en application du RGPD, l'Autorité de Protection des Données.

[51] CPVP, « note relative à la sécurité des données à caractère personnel », p. 1, disponible à l'adresse

http://www.privacycommission.be/sites/privacycommission/files/documents/note_securite_des_donnees_a_caractere_personnel.pdf

[52] Groupe 29, WP 213, *op. cit.*, p. 5. Voy égal. Groupe 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 rev. 01, 3 octobre 2017 et révisé le 6 février 2018, p. 7.

[53] La « sécurité de l'information » est, par exemple, définie comme « l'ensemble de mesures de gestion qui veillent à ce que la confidentialité, l'intégrité et la disponibilité *de toutes les formes d'information* – tant sous la forme électronique (numérique) que papier – soient maintenues, dans le but d'assurer la continuité des informations et de l'information et de limiter à un niveau acceptable prédéfini les éventuelles conséquences d'incidents en matière de sécurité de l'information ». CPVP, « Lignes directrices pour la sécurité de l'information de données à caractère personnel-Version 2.0 », décembre 2014, p. 4.

les normes internationales[54] considèrent que la sécurité a non seulement pour objectif d'assurer l'intégrité et la confidentialité des données, mais également leur disponibilité entendue comme « la propriété des informations, systèmes et processus d'être accessibles et utilisables sur demande d'une entité autorisée »[55]. La notion de disponibilité des données serait ainsi intimement liée à celle de « résilience » des réseaux et des systèmes d'information[56]. Il est donc légitime de s'interroger, d'une part, sur l'importance accordée par le RGPD à la *disponibilité d*es données à caractère personnel, et, d'autre part, sur la signification donnée par le règlement à cette propriété de sécurité considérée par le Groupe 29 comme faisant partie « des trois critères de sécurité classiques »[57].

a) Disponibilité et résilience

7. En ce qui concerne la prise en considération de ces aspects par le RGPD, un premier constat s'impose : pour la toute première fois dans le domaine de la protection des données à caractère personnel, un instrument législatif européen fait expressément référence aux *propriétés de disponibilité et de résilience* au sein de son corpus normatif. Ainsi, l'article 32, § 1, du RGPD – lequel énumère de manière non-exhaustive des moyens devant être mis en place « selon les besoins » – cite « des moyens permettant de garantir la confidentialité, l'intégrité, la *disponibilité* et la *résilience* constantes des systèmes et des services de traitement » ainsi que « des moyens permettant de rétablir la *disponibilité* des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ». Incontestablement, il s'agit là d'une nouveauté

[54] La famille de norme ISO27xxx (ISO27000 – ISO/IEC 27000 :2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary) d'un système de gestion de la sécurité (ISO27001 – ISO/IEC 27001 :2013 Information technology – Security techniques – Information security management systems – Requirements (second edition) et de diverses implémentations (ISO 27002 – ISO 27017 – ISO 27018…) est considérée comme une véritable référence dans le domaine. Un guide élaboré en janvier 2017 par la commission de normalisation AFNOR recense les normes ISO incontournables en matière de protection des données personnelles. AFNOR, « Protection des données personnelles : l'apport des normes volontaires », janvier 2017.

[55] CPVP, « note relative à la sécurité des données à caractère personnel », *op. cit.* p. 1.

[56] La résilience est l'un des fers de lance de la directive NIS pour laquelle la continuité des activités des OSE et DSP est un objectif crucial.

[57] Groupe 29, WP 213, *op. cit.*, p. 5. Le Groupe s'inspire clairement de l'ISO/CEI 27001 qui insiste particulièrement sur le triptyque « Disponibilité – Intégrité – Confidentialité ». L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. Publiée en octobre 2005 et révisée en 2013, son titre est « Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences ». Elle fait partie de la suite ISO/CEI 27000 et permet de certifier des organisations.

puisque de telles références n'apparaissent ni dans la Convention n° 108, ni dans la Directive. Clairement, cette innovation témoigne du fait que le législateur considère la *continuité de certains traitements* comme étant nécessaires à la protection de la vie privée des personnes concernées.

Pour mieux cerner la manière dont ces exigences doivent être interprétées, il nous semble utile d'évoquer deux exemples qui, pour le Groupe 29, illustrent une certaine *granularité des exigences de disponibilité* selon « les besoins »[58]. Le Groupe évoque l'hypothèse d'un hôpital dans lequel des données médicales critiques relatives à des patients sont temporairement indisponibles pouvant potentiellement conduire à l'annulation d'opérations cliniques et mettre la vie desdits patients en danger. Il imagine ensuite le cas d'une société dans le secteur des médias empêchée de communiquer des newsletters à ses abonnés suite à une attaque par déni de service[59] (ci-après « DDoS ») ou à cause d'une simple coupure de courant. Dans la première situation, « des moyens permettant de garantir la confidentialité, l'intégrité, la *disponibilité* et la *résilience* constantes des systèmes et des services de traitement » sont fortement recommandables au vu de la susceptibilité d'un risque élevé pour les personnes concernées en cas de discontinuité – même « temporaire » – du service ; dans la seconde, « des moyens permettant de rétablir la *disponibilité* des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique » seront très vraisemblablement considérés comme suffisants. Malheureusement, le Groupe s'est pour l'instant abstenu d'illustrer des cas de figure d'indisponibilité temporaires se situant dans l'échelle de gravité sans pour autant atteindre les antipodes mentionnés. Pensons, par exemple, à la vague de DDoS revendiqués par « Down-Sec Belgium » en 2015 et 2016 ayant perturbé les sites internet du Premier ministre, du Sénat, du Comité P, de la N-VA, du cdH, de BNP Paribas Fortis, de l'Office national de l'Emploi, de la Fédération Wallonie-Bruxelles, de l'Agence Fédérale de Contrôle Nucléaire ou encore de Belgocontrol, parmi de nombreux autres dont Tax-on-Web. Certes, ces incidents n'eurent pas pour conséquence de porter atteinte à l'intégrité et à la confidentialité des données traitées, mais il semble néanmoins raisonnable, par exemple, de considérer que l'atteinte à la continuité d'un service permettant aux personnes physiques d'introduire leur déclaration fiscale en ligne est susceptible d'entraîner pour celles-ci un risque pour

[58] Groupe 29, WP 250, *op. cit.*, p. 9.

[59] Une attaque par déni de service est une tentative concertée de rendre un ordinateur ou un élément de réseau indisponibles à leurs utilisateurs autorisés, que ce soit temporairement ou indéfiniment (par exemple, en utilisant de nombreux systèmes d'intrusion, qui paralysent leur cible en lançant de multiples demandes de communication externe).

leurs droits et libertés pouvant potentiellement avoir pour répercussions dommageables des pertes financières ou du moins un léger préjudice sous la forme d'une perte de temps et de désagrément[60].

b) Les violations de disponibilité temporaires

8. Le précédent exemple soulève la question de l'étendue des violations de disponibilité des données qui doivent être notifiées à l'APD conformément à l'article 33 du règlement et communiquées aux personnes concernées dans les circonstances visées à l'article 34. Dans un premier avis datant de 2014, le Groupe 29 estimait que la notion de « violation de la disponibilité » renvoyait à « la destruction ou à la perte, accidentelles ou illicites, de données à caractère personnel »[61]. Ce premier avis avait pour mérite d'avoir consciencieusement aligné les contours de la propriété de disponibilité des données sur les éléments de la définition des « violations de données à caractère personnel »[62] qui doivent lui être notifiées dans les cas prévus à l'article 33 du RGPD. Néanmoins, un certain flou régnait toujours quant à savoir si devaient ou non être communiquées aux personnes concernées des incidents ayants des effets disruptifs importants susceptibles d'entraîner des risques élevés pour celles-ci dans les cas où ces incidents n'entraînent pas de destruction ou de perte définitives de données à caractère personnel[63]. Cette interrogation ne manqua pas d'être relevée par le Groupe 29 dans les termes suivants : « *Whereas determining if there*

[60] Heureusement, parallèlement au RGPD, la directive NIS (précitée) impose aux OSE et aux DSP de nouvelles obligations en matière de sécurité des réseaux et des systèmes d'information et de notification qu'il y'ait ou non traitements de données à caractère personnel. En effet, contrairement au règlement, dont l'objectif est d'établir des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, la directive NIS a pour objet de mettre en place des mesures en vue en vue d'assurer la continuité de ces services. En cas de traitement de données à caractère personnel, les OSE et les DSP sont tenus de respecter la directive NIS et le RGPD de manière cumulative.

[61] À titre illustratif, le Groupe 29 évoquait l'hypothèse de quatre ordinateurs portables volés dans un établissement de soins contenant des données relatives à la santé de 2050 enfants. Selon le Groupe, une telle violation de la disponibilité des données pourrait avoir les conséquences et effets néfastes potentiels suivants : « elle peut troubler la continuité du traitement des enfants, entraînant l'aggravation de la maladie ou une rechute ; elle peut entraîner un empoisonnement accidentel en raison d'une allergie à un médicament ou de médicaments incompatibles, ce qui peut causer plusieurs problèmes de santé, voire le décès ; elle peut entraîner un retard excessif dans les remboursements ou l'assistance financière accordés aux personnes concernées, ce qui aurait des retombées financières pour les familles concernées ». Groupe 29, WP 213, *op. cit.*, p. 6.

[62] Art. 4, 12), du RGPD.

[63] La question se posait également pour la notification de tels incidents à l'APD dans les cas précisés en application de l'article 33, § 1, du RGPD.

has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data. The question may be asked whether a temporary loss of availability *of personal data should be considered as a breach and, if so, one which needs to be notified* »[64].

Pour cette raison, dans un avis plus récent de février 2018, le Groupe 29 révisa quelque peu le contour de la notion de « violation de la disponibilité » en la définissant comme englobant, non seulement la destruction et la perte accidentelles ou illicites de données à caractère personnel, mais également *la perte d'accès* accidentelle ou non-autorisée à celles-ci[65]. Le Groupe justifia cette adaptation en considérant que *« it is well established that "access" is fundamentally part of "availability"* » en se basant sur une définition établie par le National Institute of Standards and Technology[66] selon laquelle la propriété de disponibilité garantit également « *timely and reliable access to and use of information* »[67]. Le Groupe s'aligne ainsi sur la définition qu'il avait utilisée dans son avis de 2012 relatif au Cloud computing dans lequel « assurer la disponibilité, c'est garantir un accès fiable et en temps opportun aux données à caractère personnel »[68]. Évidemment, une indisponibilité temporaire de données résultant d'une opération de maintenance programmée ne relève pas de la définition de violation de sécurité au sens de l'article 4, 12), du règlement. Par contre, un incident illicite ou accidentel ayant pour conséquence une indisponibilité temporaire de données à caractère personnel devrait *toujours être considéré comme étant un type de violation* de sécurité dès lors qu'il est susceptible d'avoir une incidence sur les droits et libertés des personnes concernées. Par conséquent, à l'instar des autres types de violations de sécurité, une violation temporaire de disponibilité doit être documentée par le responsable du traitement, lequel doit indiquer les faits concernant l'indisponibilité temporaire des données à caractère personnel, ses effets et les mesures prises pour y remédier[69].

---

[64] Groupe 29, WP 250, *op. cit.*, p. 8.

[65] *Ibid*, p. 7.

[66] Le National Institute of Standards and Technology, ou NIST (qu'on pourrait traduire par « Institut national des normes et de la technologie »), est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.

[67] Le Groupe 29 cite NIST SP800-53rev4 dans son WP 250, *op. cit.*, p. 7.

[68] Groupe 29, WP 196, *op. cit.*, p. 17.

[69] Art. 33, § 5, du RGPD.

§ 3. Quid de l'imputabilité, de l'authenticité et de la non répudiation des données ?

a) Notions

9. Outre ces considérations relatives à la signification et à la place réservée par le RGPD à la propriété de disponibilité des données, il importe de rappeler que les trois critères de sécurité classiques (intégrité, confidentialité, disponibilité) sont traditionnellement compris comme étant des « finalités de base auxquelles s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiation d'une transaction, voire d'imputabilité) »[70].

En ce qui concerne les fonctions d'*imputabilité,* d'*authenticité* et de *non répudiation* des données, il n'est pas inutile de rappeler que l'objet du principe édicté par l'article 5, § 1, f), doit être interprété conformément aux développements jurisprudentiels en la matière. Cette remarque découle de la lecture du considérant n° 39 du règlement lequel estime que les données à caractère personnel devraient être traitées de manière à garantir une « sécurité et une confidentialité » appropriées, « y compris *pour prévenir* l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement ». À s'en tenir à la lettre dudit considérant, le RGPD ne prévoirait que l'obligation de prendre des mesures de sécurité *préventives* afin de garantir la protection des données contre les traitements non autorisés, que ceux-ci soient accidentels ou illicites : « ceci signifierait que le responsable du traitement ne serait pas obligé de prendre des mesures de sécurité *a posteriori*, comme, par exemple, des mesures de contrôle. Pour le dire autrement, la prévention des usages (traitements) non autorisés de données à caractère personnel n'imposerait que la mise en place de polices d'accès, mais pas de *log files*, ces derniers répondant en ce sens à une mesure de contrôle, c'est-à-dire à une mesure de sécurité *a posteriori* »[71]. Bref, *la fonction d'authenticité* serait incluse dans l'objet

[70] S. Ghernaouti, *Sécurité informatique et réseaux*, Paris, Dunod, 2013, p. 1. La CPVP va dans le même sens en affirmant que « dans le contexte normatif, la sécurité de l'information recouvre par définition l'obtention et la conservation de la confidentialité, de l'intégrité, de la disponibilité, de l'imputabilité, de l'authenticité, de la fiabilité et de la non répudiation de l'information et des équipements de traitement de l'information », CPVP, « note relative à la sécurité des données à caractère personnel », *op. cit.* p. 1.

[71] J. Herveg, « L'accès du patient aux log files de son dossier informatisé », *D.C.C.R.*, 2011, liv. 90, p. 44.

de l'article 5, § 1, f), du RGPD contrairement à celle *d'imputabilité* qui en serait exclue. Néanmoins, ainsi que le souligne à raison J. Herveg, « cette interprétation, même si elle peut se prévaloir d'arguments tirés d'une lecture (trop) littérale des textes, ne nous paraît pas devoir être retenue. En effet, il ne peut être sérieusement contesté que les *log files* représentent une mesure de sécurité majeure dans les traitements de données à caractère personnel, fut-ce par leur effet dissuasif à l'encontre des contrevenants potentiels, et qui ne se conçoit que liée à un système performant d'identification des personnes et de leurs actions »[72].

Et pour cause, il découle d'éclaircissements jurisprudentiels intéressants sur la portée du principe de sécurité « que les mesures de sécurité doivent non seulement empêcher les accès non autorisés [et accidentels] mais également permettre aux personnes concernées de contrôler les accès aux données qui ont eu lieu. Seul cet accès aux données sur les personnes ayant accédé aux données permet en effet à la personne concernée de vérifier *l'effectivité des mesures de sécurité* et lui permet d'exercer son contrôle ou sa maîtrise sur ses propres informations »[73]. Ainsi que C. de Terwangne le souligne, c'est en ce sens qu'a jugé la Cour européenne des droits de l'homme dans l'affaire *I c. Finlande*, condamnant cet État pour avoir laissé un hôpital public mettre en place un système de sécurité des données qui ne conserve en mémoire que les traces des cinq derniers accès aux données et qui, de surcroît efface toute trace d'accès une fois les données versées aux archives[74]. Dans le cas d'espèce, la Cour avait estimé que ce qui était requis en premier lieu est une *protection réelle et effective* qui exclut toute possibilité d'accès non autorisé afin d'obtenir une indemnisation pour le dommage causé par une divulgation non autorisée de données à caractère personnel[75]. Dans la même ligne, la Cour de justice de l'Union européenne a rappelé dans son arrêt *Rijkeboer*[76] que la personne concernée devait non seulement pouvoir obtenir réparation pour le dommage subi du fait d'un

[72] *Ibid.*

[73] C. de Terwangne, « La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 113.

[74] Cour eur. D.H., 17 juillet 2008, *I. v. Finlande*, req. n° 20511/03, § 41.

[75] Cour eur. D.H., 17 juillet 2008, *I. v. Finlande*, req. n° 20511/03, § 47.

[76] C.J.U.E., 7 mai 2009, arrêt *College van burgemeester en wethouders van Rotterdam c. M. E.E. Rijkeboer*, C-553/07. « Dans cette affaire, M. Rijkeboer avait demandé au Collège de Rotterdam de l'informer de tous les cas où des informations le concernant et provenant de l'administration communale avaient été communiquées à des personnes tierces au cours des deux années précédant sa demande. Il désirait connaître l'identité de ces personnes et le contenu de l'information qui leur avait été transmise. Il avait déménagé dans une autre commune et souhaitait savoir, en particulier, à qui son ancienne adresse avait été communiquée. Il n'a reçu de réponse que pour l'année précédant sa demande, les données antérieures

traitement illicite mais également disposer d'un recours juridictionnel en cas de violation des droits qui lui étaient reconnus[77]. Pour cette raison, la Cour estima que pour *assurer* un *effet utile*, le droit d'accès concerne nécessairement le passé[78] : « en effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer *de manière efficace* son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi »[79]. C. de Terwangne ajoute que la protection des données « implique que la personne concernée *puisse s'assurer que ses données à caractère personnel sont adressées à des destinataires autorisés*. Afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Cela implique l'obligation de conservation pendant une certaine durée des renseignements relatifs aux personnes destinataires des données ainsi qu'aux données précisément consultées ou transmises »[80]. La lecture de ces développements jurisprudentiels suggère donc que la portée du principe de sécurité sous le régime du RGPD puisse englober – « selon les besoins » – les fonctions d'*authenticité, d'imputabilité*, mais également de *non répudiation* des données. En effet, les deux premières propriétés citées n'auraient aucun effet utile à défaut d'un mécanisme permettant de démontrer qu'un accès non autorisé a bien eu lieu sans qu'il puisse être nié ultérieurement.

b) Des fonctions de sécurité parfois légalement reconnues

10. Le RGPD ne consacre pas explicitement les fonctions d'imputabilité, d'authenticité et de non répudiation des données, pourtant considérées par la jurisprudence européenne comme étant nécessaires à l'effectivité des trois propriétés de sécurité classiques. Néanmoins, lesdites fonctions de sécurité sont déjà expressément reconnues par d'autres instruments législatifs en matière de protection des données à caractère personnel ;

---

ayant été automatiquement effacées conformément à la loi des Pays-Bas relative aux données personnelles détenues par les administrations communales ». Voy. J. Herveg, « L'accès du patient aux log files de son dossier informatisé », *op. cit.*, p. 49.

77 C.J.U.E., arrêt *Rijkeboer,* préc., § 18.

78 Voy. sur ce point C. de Terwangne, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 7 mai 2009, *R.D.T.I.*, 2011, n° 43, pp. 65-81.

79 C.J.U.E., arrêt *Rijkeboer*, *op. cit.*, § 54.

80 C. de Terwangne, « La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 113.

parfois en raison de la sensibilité du contexte qu'ils régulent, parfois de manière plus horizontale[81].

Il en va ainsi tout d'abord dans le domaine médical dans lequel la Cour européenne des droits de l'Homme estima dès 1997 que « la législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention »[82]. Partant, la même année, le Conseil de l'Europe adopta la Recommandation n° R(97)5 relative à la protection des données médicales[83] qui contient en son point 9 une imposante énumération des mesures qui devraient être prises pour assurer un niveau de sécurité « approprié » dans le dit contexte : contrôle à l'entrée des installations, contrôle des supports de données, contrôle de mémoire, contrôle de l'utilisation, contrôle d'accès, contrôle de la communication, contrôle de l'introduction et contrôle du transport[84].

De même, dans le cadre de la « directive police »[85], l'article 29, § 2, prévoit que le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées au contrôle de l'accès aux installations, au contrôle des supports de données, au contrôle de la conservation, au contrôle des utilisateurs, au contrôle de l'accès aux données, au contrôle de la transmission, au contrôle de l'introduction et au contrôle du transport[86]. De plus, l'article 25 de ladite directive régule spécifiquement la journalisation en prévoyant que « les États membres prévoient que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la

[81] Nous ne prétendons établir aucune liste exhaustive des instruments particuliers prévoyant des obligations ou des recommandations additionnelles en matière de sécurité informationnelle. Les exemples énumérés ne le sont qu'à titre purement illustratif.

[82] Cour eur. D.H., *Z. c Finlande*, 25 février 1997, req. n° 22009/93, § 95.

[83] Conseil de l'Europe, Recommandation n° R (97) 5 du Comité des ministres aux États membres relative à la protection des données médicales, adoptée le 13 février 1997.

[84] Outre les mesures de contrôles énumérées, la Recommandation n° R (97) 5 préconise également l'établissement d'un règlement interne approprié et, « si nécessaire », la désignation d'une personne indépendante responsable de la sécurité des systèmes d'information et de la protection des données.

[85] Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[86] Voy. l'article 29, § 2, de la directive 2016/680/UE pour une définition de ces mesures de contrôle.

collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel »[87].

De manière analogue, en ce qui concerne l'utilisation des données à caractère personnel par les institutions et organes de l'UE, l'article 22 du règlement 45/2001[88] prévoit que des mesures sont prises lorsqu'elles sont nécessaires au regard des risques encourus et énumère le même type de mesures de contrôle[89].

[87] Pour le surplus, l'article 25, § 2, de la directive 2016/680/UE précise que « les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales ». Le paragraphe 3 dudit article précise, quant à lui, que « le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle, sur demande ».

[88] Règlement (CE) 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

[89] Telles des mesures prises « dans le but : a) d'empêcher toute personne non autorisée d'avoir accès aux systèmes informatiques de traitement des données à caractère personnel ; b) d'empêcher que des supports de stockage puissent être lus, copiés, modifiés ou déplacés sans autorisation ; c) d'empêcher toute introduction non autorisée de données dans la mémoire ainsi que toute divulgation, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées ; d) d'empêcher des personnes non autorisées d'utiliser des systèmes de traitement de données au moyen d'installations de transmission de données ; e) de garantir que les utilisateurs autorisés d'un système de traitement des données ne puissent accéder qu'aux données à caractère personnel que leur droit d'accès leur permet de consulter ; f) de garder une trace des données à caractère personnel qui ont été communiquées, du moment où elles l'ont été et de leur destinataire ; g) de garantir qu'il sera possible de vérifier a posteriori quelles données à caractère personnel ont été traitées, à quel moment et par quelles personnes ; h) de garantir que des données personnelles qui sont traitées pour le compte de tiers ne peuvent l'être que de la façon prévue par l'institution ou l'organe contractant ; i) de garantir que, lors de la communication de données à caractère personnel et du transport de supports de stockage, les données ne puissent être lues, copiées ou effacées sans autorisation ; j) de concevoir la structure organisationnelle interne d'une institution ou d'un organe de manière à ce qu'elle réponde aux exigences propres à la protection des données ».

SECTION 2. – La sécurité du réseau et des informations : un intérêt légitime

§ 1. Objet

11. Outre les cas dans lesquels l'imputabilité, l'authenticité et la non répudiation des données sont légalement requises ou recommandées, il va sans dire que la *mise en œuvre strictement nécessaire et proportionnée* de ces trois fonctions de sécurité s'avèrera utile à des fins probatoires dans le cadre de potentielles procédures civiles, disciplinaires, administratives ou pénales, notamment lorsque la licéité d'un accès aux données est contestée ou lorsqu'une violation de données à caractère personnel est en jeu. De toute évidence, il est de l'intérêt de la justice que la capacité d'une personne d'agir pour promouvoir ou défendre un droit reconnu par la loi ne soit pas *disproportionnellement* restreinte et qu'elle puisse se réserver des preuves à cet effet. La mise en œuvre *proportionnée* de ces fonctions de sécurité peut également être conseillée afin de respecter le principe d'*accountability* envers les autorités de contrôle en cas de violation de données.

Les trois mesures de sécurité susmentionnées ont toutefois comme particularité d'être elles-mêmes des traitements de données à caractère personnel, lesquelles sont par conséquent soumises au régime du RGPD, notamment en termes de nécessité, de proportionnalité, de finalité, de transparence, de droits, de minimisation, de durée de conservation et de sécurité. Pour ce qui concerne leur *fondement de licéité*, le consentement des personnes concernées n'est toutefois pas nécessaire, l'intérêt légitime du responsable du traitement ou d'un tiers[90] autorisé à traiter les données étant suffisant[91].

En effet, le considérant n° 49 du RGPD stipule explicitement que « le traitement de données à caractère personnel dans la mesure *strictement*

[90] Art. 4, 10), du RGPD. Un « tiers » est défini comme étant « une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ».

[91] L'article 6 du RGPD n'autorise le traitement de données à caractère personnel que si au moins un des six fondements juridiques énumérés audit article s'applique. Parmi ceux-ci, l'article 6, § 1, f), du règlement stipule que le traitement est licite lorsqu'il « est *nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers*, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel […] ». Autrement dit, ledit « fondement de licéité » autorise le traitement, sous réserve d'une mise en balance qui compare l'intérêt légitime poursuivi par le responsable du traitement – ou par le ou les tiers auxquels les données sont communiquées – avec l'intérêt ou les droits fondamentaux des personnes concernées.

nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations […] constitue un intérêt légitime du responsable du traitement concerné ». La notion de « sécurité du réseau et des informations » y est par ailleurs définie comme étant « la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la *disponibilité*, *l'authenticité*, *l'intégrité* et *la confidentialité* de données à caractère personnel conservées ou transmises ». Sont également considérés comme relevant de l'intérêt légitime, « la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité ». L'objectif serait, entre autres, « d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par DDoS et des dommages touchant les systèmes de communications informatiques et électroniques ».

Dans le même esprit, le considérant n° 50 du RGPD stipule que « le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement »[92].

À cet égard, il n'est pas inutile non plus de rappeler que « les autorités publiques auxquelles des données à caractère personnel sont communiquées conformément à une obligation légale pour l'exercice de leurs fonctions officielles […] ne devraient pas être considérées comme des destinataires si elles reçoivent des données à caractère personnel qui sont nécessaires pour mener une enquête particulière dans l'intérêt général, conformément au droit de l'Union ou au droit d'un État membre »[93]. Par conséquent, les transmissions de données ponctuelles et proportionnées

[92] Néanmoins, cette transmission dans l'intérêt légitime du responsable du traitement ou le traitement ultérieur des données à caractère personnel devrait être interdit lorsque le traitement est incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante.

[93] Considérant n° 50 du RGPD. Néanmoins, « les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel

aux autorités européennes[94] susmentionnées dans le cadre strict de leurs missions légales ne devraient pas être mentionnées dans le Registre des activités de traitement tel que régi par l'article 30 du RGPD.

Pour ce qui est des interactions entre les débiteurs de l'obligation de sécurité et les autorités susmentionnées, la Convention de Budapest[95] prévoient des méthodes d'enquêtes spécifiques pour les forces de l'ordre dans le contexte digital, dont notamment l'identification, le repérage, la saisie de données informatiques, la recherche dans un système informatique et l'interception de communications[96]. En ce qui concerne notre propos, il est important de mentionner que la collaboration d'un responsable du traitement ou d'un sous-traitant peut également être exigée par ces autorités. À titre d'exemple, en Belgique, une telle collaboration peut être demandée sur base d'une ordonnance du juge d'instruction conformément aux articles 88*bis* et 90*quater* du Code d'instruction criminelle (ci-après « CICr »)[97]. Le refus de collaboration et le refus de prêter un concours technique sont passibles de sanctions pénales. Ces considérations ne sont pas sans intérêt pour les débiteurs de l'obligation de sécurité puisque dans un arrêt récent, Skype – devant collaborer en vue de permettre l'interception des données de communications électroniques – invoquait l'impos-

---

par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement ». Voy. égal. la définition de « destinataire » à l'article 4, 9), du RGPD.

[94] Cependant, relevons qu'une obligation imposée par une loi ou un règlement étranger ne saurait être qualifiée d'obligation légale légitimant le traitement de données dans l'Union européenne. Toutefois, dans chaque État membre, une obligation légale peut imposer l'exécution d'une ordonnance d'une juridiction d'un autre État demandant un tel échange d'informations. De plus, la conformité aux exigences de la procédure judiciaire d'un pays tiers peut s'avérer nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées. Ce motif serait acceptable « à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ». Voy. not. Groupe 29, Document de travail 1/2009 sur la procédure d'échange d'informations avant le procès (« pre-trial discovery ») dans le cadre de procédures civiles transfrontalières, WP 158, 11 février 2009, pp. 10 et 11.

[95] Conseil de l'Europe, Convention sur la cybercriminalité (STE n° 185), Budapest, 23 novembre 2001.

[96] Pour une analyse de ces méthodes d'enquête, lire C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique, vers un cadre (plus) strict ? », *R.D.T.I.*, n° 66-67, 2017, pp. 25-52, 2018.

[97] En Belgique, afin de pouvoir intercepter les communications, le juge d'instruction peut requérir directement ou par l'intermédiaire du service de police désigné par le Roi, le concours « en temps réel » *de toute* personne présumée disposer de connaissance particulière du système informatique qu'elles fournissent des informations sur le fonctionnement de ce moyen ou système et sur la manière d'accéder à son contenu qui est ou a été transmis, dans une forme compréhensible. Il peut ordonner aux personnes de rendre accessible ce contenu, dans la forme qu'il souhaite, notamment dans le cas où celui-ci est chiffré. Art. 90*quater*, § 4, CICr.

sibilité matérielle de prêter son concours en raison du chiffrement des données[98]. Selon la cour d'appel, en créant ses services, Skype aurait dû tenir compte des obligations de collaboration découlant du droit national belge. Cette interprétation peut sembler entrer en résonnance avec les concepts de « *privacy by design* » ou de « *privacy by default* » qui imposent au responsable du traitement de prendre en considération, dès la conception, la nécessité de mettre en œuvre des mesures techniques et organisationnelles appropriées[99]. Cependant, la question mérite d'être posée quant à savoir si ces approches vont jusqu'à leur imposer des obligations de « *collaboration by design* » avec les autorités policières et judiciaires. À cet égard, le Groupe 29 a encore récemment rappelé que « *encryption must remain standardized, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys. Whatever the technical solution, it can never be safe to compel encryption providers to include master keys and backdoors in their software. Law enforcement agencies already have access to vast quantities of data via their existing powers. Such access must remain proportionate and targeted. They should focus on improving their capabilities to interpret those data to investigate and prosecute criminals* »[100].

Néanmoins, insistons sur le fait que l'anonymat est loin d'être un droit absolu pour les personnes concernées et que les États ont l'obligation positive, inhérente à l'article 8 de la CEDH, d'adopter des dispositions en matière pénale qui sanctionnent effectivement les infractions contre les personnes[101]. Dans l'arrêt *K.U. c. Finlande*, la Cour a ainsi estimé qu'une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier l'auteur[102]. De manière similaire, dans un arrêt du 15 septembre 2016, la Cour de Justice de l'Union européenne a estimé que le droit européen ne s'oppose pas à l'adoption d'une injonction judiciaire consistant à exiger d'un fournisseur d'accès à un réseau accessible au public de sécuriser la connexion à Internet au moyen d'un mot de passe afin que les utilisateurs de ce réseau soient obligés de révéler leur identité et ne puissent donc pas agir anonymement[103].

---

[98] Anvers (4e ch.) n° 2016/CO/1006, 15 novembre 2017, inédit.

[99] Art. 25 du RGPD.

[100] Groupe 29, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, 11 avril 2018, p. 3.

[101] Cour eur. D.H., *M.C. c. Bulgarie*, 4 décembre 2003, req. n° 39272/98, § 150.

[102] Cour eur. D.H., *K.U. c. Finlande*, 2 décembre 2008, req. n° 2872/02, § 49. Dans cette affaire, le requérant se plaignait qu'une annonce à caractère sexuel ait été publiée à son sujet sur un site de rencontres par Internet et que la législation finlandaise en vigueur à l'époque n'ait pas permis à la police et aux tribunaux d'obliger le fournisseur d'accès à identifier l'auteur de l'annonce.

[103] C.J.U.E., 15 septembre 2016, arrêt *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, C-484/14, § 102.

§ 2. L'enjeu de la journalisation

12. Si l'on peut féliciter le législateur européen d'avoir consolidé l'obligation de sécurité, on peut toutefois regretter que le RGPD n'ait pas explicitement précisé les facteurs à prendre en compte pour évaluer *la nécessité et la proportionnalité* des traitements de données à des fins de journalisation. Une clarification des principes applicables, notamment, au contenu, à la durée de conservation, aux accès et aux finalités des « journaux de sécurité », également appelés « logfiles » ou « logs »[104] aurait été plus qu'utile.

En effet, il s'agit là d'en enjeu crucial. D'une part, le respect des droits fondamentaux et l'intérêt légitime de la cybersécurité ne peuvent se concevoir sans une lutte effective, mais proportionnée contre la cybercriminalité ; d'autre part, le contrôle disproportionné par les employeurs des données de communication de leurs travailleurs reste un problème récurrent[105]. En effet, le droit matériel réprime les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données[106]. Par ailleurs, le droit pénal procédural prévoit des compétences d'enquête dans le contexte digital. Enfin, la Cour européenne des droits de l'Homme fixe certains principes de proportionnalité du contrôle des données de communication électroniques dans le cadre de la relation de travail[107]. Dans ce contexte, un cadre légal régissant de manière explicite la journalisation aurait été le bienvenu afin, d'une part, de garantir une certaine sécurité juridique vis-à-vis des personnes concernées qui exerceraient leur *droit d'accès pour le passé* et, d'autre part, de préciser les exigences qu'ont les débiteurs de l'obligation de sécurité vis-à-vis des autorités policières, judiciaires – et/ou les CERT –. Cela aurait permis d'expliciter les contours de la fonction d'imputabilité, « cette propriété qui permet de pouvoir identifier, pour toutes les actions accomplies, les personnes, les

[104] Un « log », « logfile » ou encore « fichier journal » est un fichier contenant des événements se produisant au sein des systèmes d'information et réseaux d'une organisation. Ces logs peuvent être générés par de multiples applications, comme par exemple un système d'exploitation, un antivirus, un firewall, un système de détection d'intrusion ou de prévention, et, de manière plus générale, par n'importe quel programme installé sur un serveur, un poste de travail ou un équipement de réseautique. NIST, *Guide to Computer Security Log Management*, Septembre 2006, p. 9.

[105] Groupe 29, Avis 2/2017 sur le traitement des données sur le lieu de travail, WP 249, 8 juin 2017. Voy. égal. Groupe 29, Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel, WP 48, 13 septembre 2001 et Groupe 29, Document de travail concernant la surveillance des communications électroniques sur le lieu de travail, WP 55, 29 mai 2002.

[106] Voy. par exemple, les articles 2 à 6 de la Convention de Budapest.

[107] Cour eur. D.H. (GC), arrêt *Bărbulescu c. Roumanie*, 7 septembre 2017, req. n° 61496/08.

systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) »[108].

13. Des précisions quant à la *nécessité et la proportionnalité* de la journalisation peuvent toutefois être trouvées dans les mesures de référence de la CPVP *applicables à tout traitement de données à caractère personnel*[109]. *Dans celles-ci l'APD nationale belge prend position en recommandant à tous* les débiteurs de l'obligation de sécurité de mettre en œuvre des mécanismes « qui doivent permettre de retrouver, en cas de nécessité, l'identité de l'auteur de tout accès aux données à caractère personnel ou de toute manipulation de celles-ci. L'enregistrement de ces informations de contrôle peut concerner, *suivant les cas*, l'accès physique, l'accès logique ou les deux. La granularité des enregistrements, la localisation et la durée de conservation de ceux-ci, la fréquence et le type des manipulations effectuées sur ceux-ci dépendent du contexte ». La CNIL adopte le même type de recommandation en estimant qu'« afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés. Dans tous les cas, il ne faut pas conserver ces éléments pendant une durée excessive »[110]. Dans le même document, la CNIL énumère les précautions nécessaires à prendre en compte lors de la mise en œuvre de la journalisation[111].

---

[108] CPVP, « note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 2.

[109] CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel - version 1.0 », p. 4, disponible à l'adresse https://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf.

[110] CNIL, « La sécurité des données personnelles », *Les guides de la CNIL*, édition 2017, p. 10, disponible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf.

[111] *Ibid.* Selon la CNIL, « il s'agit de « prévoir un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité : ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ; la journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ; dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné. Il faut informer les utilisateurs de la mise en place d'un tel système, après information et consultation des représentants du personnel ;

De fait, il s'agit de ne pas confondre la finalité de journalisation avec celle de la surveillance des employés en utilisant, par exemple, les *logs* pour évaluer leur rentabilité. Une telle *autre* finalité pose en effet la délicate question de « l'équilibre entre l'intérêt légitime de l'employeur à protéger ses activités et les attentes raisonnables des personnes concernées, à savoir les employés, en matière de respect de la vie privée »[112]. À cet égard, rappelons que la directive 2002/58/CE[113] précise que le principe de confidentialité s'applique tant au contenu des communications qu'à toutes « données afférentes » à celles-ci[114], y compris les données de trafic[115] et de localisation[116]. Ces dernières sont effectivement « susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les

protéger les équipements de journalisation et les informations journalisées contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée ; établir des procédures détaillant la surveillance de l'utilisation du traitement et examiner périodiquement les journaux d'événements pour y détecter d'éventuelles anomalies ; assurer que les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement ; et enfin notifier toute violation de données à caractère personnel à la CNIL et, sauf exception prévue par le RGPD, aux personnes concernées pour qu'elles puissent en limiter les conséquences ».

[112] Groupe 29, WP 249, *op. cit.*, p. 4. Dans le cadre de cette contribution, nous n'analysons pas en détail la problématique de la protection des données à caractère personnel des employés dans le contexte du travail.

[113] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). Ladite directive est du reste en voie de révision. Voy. Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE, 2017/0003 (COD).

[114] Considérant n° 21 de la directive 2002/58/CE : « Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, y compris de leur contenu et de toute donnée afférente à ces communications ».

[115] Art. 2, b), de la directive 2002/58/CE selon lequel les « données relatives au trafic » sont toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation.

[116] Art. 2, c), de la directive 2002/58/CE selon lequel les « données de localisation » sont toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ; les abonnés devraient disposer d'un moyen simple pour interdire temporairement le traitement des données de localisation et ce, gratuitement.

relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir […] le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications »[117]. Ces considérations peuvent être prises en compte dans le contexte professionnel dans lequel « le contenu [et les données de trafic][118] des communications électroniques effectuées à partir de locaux professionnels bénéficie des mêmes protections des droits fondamentaux que les communications analogiques »[119].

14. Enfin, les données de traçage étant elles-mêmes des données à caractère personnel, tout traitement de celles-ci doit se conformer au RGPD et s'accompagner des mesures de sécurité adéquates[120], conformément à l'approche développée dans les sections suivantes[121].

---

[117] C.J.U.E., 21 décembre 2016, arrêt *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.,* affaires jointes C-203/15 et C-698/15, § 99.

[118] Cette approche est corroborée par l'article 4, 1), du RGPD – lequel liste expressément les identifiants en ligne et les données de localisation dans la définition du concept de « données à caractère personnel – et confirmée par le considérant n° 30 selon lequel « les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes ».

[119] Groupe 29, WP 249, *op. cit.*, p. 3. Voy. aussi Cour eur. D.H., 3 avril 2007, *Copland c. Royaume-Uni*, req. n° 62617/00 dans laquelle la Cour a déclaré que les courriers électroniques envoyés à partir de locaux professionnels et les informations découlant de la surveillance de l'utilisation de l'internet pouvaient faire partie de la vie privée et de la correspondance d'un employé, et que la collecte et la conservation de ces informations à l'insu de l'employé constitueraient une atteinte à ses droits, bien que la Cour n'ait pas statué qu'une telle surveillance ne serait jamais nécessaire dans une société démocratique. Voy. égal. Cour eur. D.H., 5 septembre 2017, *Bărbulescu c. Roumanie*, req n° 61496/08 dans laquelle la Cour précise les critères que doivent appliquer les autorités nationales lorsqu'elles apprécient si une mesure prise pour surveiller les communications des employés est proportionnée au but poursuivi et si l'employé concerné est protégé contre l'arbitraire.

[120] CPVP, Mesures de référence applicables à tout traitement de données à caractère personnel, *op. cit.*, p. 5.

[121] À titre indicatif, le Groupe 29 mentionne explicitement « la technologie eDiscovery, qui désigne tout processus dans lequel des données électroniques font l'objet d'une recherche dans le but de les utiliser comme éléments de preuve » comme étant un traitement de données à caractère personnel devant respecter lesdits principes. Voy. Groupe 29, WP 249, *op. cit.*, p. 15.

CHAPITRE 3. L'obligation renforcée de sécurité des traitements

SECTION 1. – Objet de l'obligation

15. Pour saisir la portée de l'obligation de sécurité, il faut se pencher sur une série d'exigences reprises dans le RGPD qui participent toutes à l'objectif d'amener les responsables de traitement et les sous-traitants à remplir cette obligation. Au sein de cette section, nous nous limiterons à évoquer ces différentes exigences sur lesquelles nous reviendrons de manière plus détaillée dans les sections ultérieures, l'objectif étant à ce stade de dégager une vue d'ensemble de l'objet de l'obligation de sécurité telle que schématiquement illustrée par le tableau ci-dessous.

<table>
<tr><td colspan="5">1) Recommandation méthodologique de tenir un Registre pour les traitements non-occasionnels</td></tr>
<tr><td>2) Traitement</td><td>Nature</td><td>Portée</td><td>Contexte</td><td>Finalité</td></tr>
<tr><td colspan="5">3) Risques pour les droits des personnes physiques</td></tr>
<tr><td>4) Traitement illicite/ accidentel</td><td colspan="2">5) Probabilité</td><td colspan="2">6) Gravité</td></tr>
<tr><td>• Destruction
• Perte
• Indisponibilité temporaire
• Altération
• Divulgation (non autorisée)
• Accès (non autorisé)
• Autres ?</td><td colspan="2"></td><td colspan="2"></td><td>7) Dommages</td></tr>
<tr><td></td><td colspan="3">8) Risque inhérent</td><td></td></tr>
<tr><td>Risque inhérent faible</td><td colspan="2">Doute quant au niveau du risque inhérent</td><td colspan="2">Risque inhérent élevé</td></tr>
<tr><td>Documenter l'appréciation du risque faible et ré-évaluer en permanence les risques engendrés par les activités de traitement afin de pouvoir établir qu'un type de traitements est susceptible d'engendrer un risque élevé ou non. Dans l'éventualité du premier cas, procéder à une AIPD.</td><td colspan="2">Forte recommandation de procéder à une AIPD. Le cas échéant, expliquer et documenter les motifs de la décision de ne pas procéder à une AIPD en incluant/rapportant par ailleurs l'opinion à cet égard du délégué à la protection des données.</td><td colspan="2">Obligation de procéder à une AIPD</td></tr>
</table>

État des connaissances	Couts de mise en œuvre
Mesures appropriées	
Techniques	**Organisationnelles**
• Pseudonymisation • Chiffrement • Autres ?	• Procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. • Autres ?
Techniques et organisationnelles	
• Moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement. • Moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique. • Autres ?	
Risque résiduel	
En cas de risque résiduel élevé, consulter l'autorité de contrôle préalablement au traitement.	
Violation de données ?	
Notification à l'autorité de contrôle d'une violation de données à caractère personnel à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physique.	
Communication à la personne concernée d'une violation de données à caractère personnel lorsque la violation en question est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.	

Figure 2 – Schéma de l'objet de l'obligation de sécurité des traitements

16. Tout d'abord, dans l'objectif de promouvoir la mise en œuvre d'une méthodologie documentaire respectueuse du principe d'*accountability* envers les autorités de contrôle[122], la première ligne de notre tableau recommande à tous les responsables de traitements et aux sous-traitants de tenir un Registre afin de décrire de manière détaillée leurs traitements de données non-occasionnels[123].

Cette première contrainte documentaire est un préliminaire de base puisque l'article 32, § 1, du RGPD impose d'évaluer le risque « inhérent »[124] (point 8 de notre tableau) du traitement pour les droits et libertés des personnes physiques (point 3), *dont le degré de probabilité* (point 5) et de *gravité* (point 6) varie « en fonction de la nature, de la portée, du contexte et des finalités du traitement »[125] (ligne 2 de notre tableau).

Ainsi qu'illustré par la quatrième ligne de notre tableau, l'article 32, § 2, précise que, lors de l'évaluation de la probabilité et de la gravité du risque « inhérent »[126], il doit être tenu compte en particulier des sources du risque « résultant *notamment* de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données ». Le point 7 de notre tableau illustre que de tels traitements accidentels ou illicites sont en effet susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral pour les personnes concernées, ou à tout le moins des conséquences négatives pour les libertés et droits fondamentaux de celles-ci[127].

À l'issue de cette évaluation, lorsqu'un traitement est considéré comme étant susceptible d'engendrer un « risque inhérent élevé » pour les droits et libertés des personnes physiques, l'article 35 impose au responsable du

---

[122] Selon l'article 31 du RGPD, « le responsable du traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants coopèrent avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions ».

[123] Art. 30 du RGPD.

[124] Considérant n° 83 du RGPD.

[125] Voy. égal. considérant n° 76 du RGPD.

[126] « En matière de gestion des risques, on peut en règle générale faire une distinction entre le risque « inhérent » et le risque « résiduel ». Le risque « inhérent » renvoie à la probabilité qu'un impact négatif se produise lorsqu'aucune mesure de protection n'est prise. Le risque « résiduel » « renvoie au contraire à la probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent) ». Voy. CPVP, Recommandation n° 01/2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable, 28 février 2018, p. 19. La CPVP cite par ailleurs IEC/ISO, « Risk management – Risk management techniques », IEC/ISO 31010, v1.0, 2009-11, p. 12 selon lequel « Lors de l'analyse (évaluation) du risque, on tient compte de la présence (ou de l'absence) et de l'efficacité de mesures techniques et organisationnelles qui limitent le risque ».

[127] Considérant n° 75 du RGPD.

traitement de se conformer à l'exigence d'une seconde contrainte documentaire, à savoir la conduite d'une AIPD, laquelle doit être réalisée avant la mise en œuvre du traitement envisagé[128].

Qu'une telle AIPD soit à l'origine requise/recommandée ou non, tant le responsable du traitement que le sous-traitant sont tenus d'atténuer les risques « inhérents » qu'ils ont identifiés grâce à la mise en œuvre des mesures techniques et organisationnelles appropriées dès lors qu'elle a été réalisée[129]. Outre les facteurs déjà mentionnés, ces deux types de mesures doivent tenir de compte de l'état des connaissances et des coûts de mise en œuvre afin de faire en sorte que les opérations de traitement atteignent un niveau de risque « résiduel »[130] acceptable ou tolérable. À cet égard, l'article 32, § 1, énumère, *de manière non-exhaustive*, des mesures qui peuvent être envisagées « selon les besoins », à savoir :

- la pseudonymisation et le chiffrement ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

De plus, dans l'hypothèse où une AIPD est effectuée et qu'elle indique que le traitement présenterait un « risque résiduel élevé », le responsable du traitement doit consulter l'autorité de contrôle préalablement au traitement[131].

En outre, en cas de violations de données *susceptible d'engendrer un risque* pour les droits et libertés des personnes physiques, l'article 33, § 1, du RGPD prévoit que le responsable du traitement est tenu de notifier celles-ci à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Enfin, lorsqu'une violation de données à caractère personnel est *susceptible d'engendrer un risque élevé*, le responsable du traitement doit communiquer ladite violation de données à caractère personnel à la personne concernée dans les meilleurs délais[132].

---

[128] Art. 35, § 1, du RGPD.

[129] Art. 32, § 1, du RGPD.

[130] Voy. ISO, « Risk management – Vocabulary », ISO Guide 73 :2009, qui décrit le « risque résiduel » comme « risque subsistant après le traitement du risque ».

[131] Art. 36, § 1, du RGPD.

[132] Art. 34, § 1, du RGPD.

SECTION 2. – Débiteurs de l'obligation

17. Pour ce qui est du respect du principe d'intégrité et de confidentialité prescrit à l'article 5, § 1, f), du règlement, les articles 5, § 2, et 24 prévoient que le responsable du traitement en endosse la responsabilité, tant pour tout traitement de données à caractère personnel qu'il effectue lui-même que pour ceux qui sont réalisés pour son compte[133]. Il ne peut d'ailleurs faire appel qu'à des sous-traitants qui « présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées »[134]. Qui plus est, afin de satisfaire à l'exigence d'*accountability*, le responsable du traitement doit être en mesure de démontrer que ledit principe de sécurité est respecté, en ce compris l'efficacité des mesures[135], lesquelles doivent être réexaminées et actualisées si nécessaire[136]. À ce titre, c'est également le responsable du traitement qui assume la responsabilité d'effectuer une AIPD lorsqu'une telle démarche doit être entreprise[137]. Néanmoins, « si nécessaire et sur demande », le sous-traitant doit aider le responsable du traitement, à assurer le respect des obligations découlant de la réalisation de ces AIPD[138]. À cet effet, l'article 28, § 3, f), du RGPD impose que le contrat de sous-traitance mentionne obligatoirement cette collaboration « compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ».

Le sous-traitant est d'autant plus impliqué puisque contrairement à l'article 17, § 1, de la directive 95/46/CE qui ne visait expressément que le seul responsable du traitement[139], l'article 32 du RGPD considère non

---

133 Considérant n° 74 du RGPD.

134 Art. 28, § 1, et considérant n° 81du RGPD.

135 Considérant n° 74 et art. 24 du RGPD.

136 Art. 24 du RGPD.

137 Considérant n° 84 du RGPD.

138 Considérant n° 95 du RGPD.

139 Néanmoins, relevons que l'article 17, § 2, de la Directive imposait aux États-Membres de prévoir que le responsable du traitement « doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures ». De plus, l'article 17, § 3, exige que « la réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que [...] les obligations visées au paragraphe 1, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci ». De plus, même sous le régime de la Directive, le devoir principal du responsable du traitement étant de veiller à ce que les données traitées ne le soient pas ultérieurement de manière incompatible avec les finalités déterminées initialement, il va de soi qu'en cas d'incident de sécurité impliquant une fuite de données engendrant un détournement de finalité, un sous-traitant négligeant pourrait voir sa qualification juridique réformée en responsable du traitement.

seulement le responsable du traitement mais également le sous-traitant comme débiteurs de l'obligation de sécurité. Par conséquent, en cas de manquement, leur responsabilité solidaire pourra être éventuellement engagée conformément aux articles 82 et 83 du règlement. Sur le plan administratif, la répartition des éventuelles amendes dépendra notamment de leur degré de responsabilité respectif dans la violation de l'obligation, compte tenu des mesures techniques et organisationnelles qu'ils ont chacun mises en œuvre[140]. Sur le plan civil, la personne lésée pourra, au choix, demander réparation du préjudice subi à l'un ou à l'autre[141], lequel pourra ensuite se retourner contre le partenaire contractuel en ce qui concerne sa part de responsabilité dans le dommage[142].

Autant dire qu'en cas de sous-traitance, des dispositions conventionnelles détaillées en matière de sécurité sont d'une importance cruciale pour assurer à l'un ou l'autre acteur la possibilité de prouver que le fait qui a provoqué le dommage lui est partiellement ou nullement imputable et ainsi être exonéré de responsabilité, en tout ou en partie. À cet égard, le contrat de sous-traitance doit notamment obligatoirement prévoir que :

- le sous-traitant aide le responsable du traitement à garantir le respect de l'obligation de sécurité de ce dernier compte tenu de la nature du traitement et des informations à la disposition du sous-traitant[143] ;
- le sous-traitant mette à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de son obligation de sécurité, ainsi que pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits[144].

Pour le surplus, il convient d'indiquer qu'outre les mentions imposées par l'article 28, § 3, du RGPD, rien n'empêche le contrat de sous-traitance de contenir des instructions additionnelles en matière de sécurité informationnelle auxquelles le sous-traitant devra se conformer.

SECTION 3. – Nature de l'obligation

18. La nature de l'obligation de sécurité consacrée à l'article 32 du RGPD n'est pas définie par le texte du règlement, mais étant donné que

[140] Art. 83, § 2, d), du RGPD.
[141] Art. 82, § 1, du RGPD.
[142] Art. 82, § 5, du RGPD.
[143] Art. 28 § 3, f), du RGPD.
[144] Art. 28, § 3, f) et h), du RGPD.

l'utopie du risque nul est un mythe[145], il paraît évident de la considérer comme une obligation de moyens et non de résultat[146]. Cette distinction entre obligation de résultat et obligation de moyens a un intérêt essentiel en ce qui concerne la charge de la preuve ainsi que l'étendue de la responsabilité des débiteurs d'une telle obligation. En effet, une obligation de moyens ne peut mettre en jeu la responsabilité du débiteur que si le créancier prouve que ce dernier a commis une faute en n'utilisant pas tous les moyens à sa disposition pour respecter son obligation. Par conséquent, les débiteurs de l'obligation de sécurité sont « seulement » tenus d'apporter les soins et diligences normalement nécessaires pour atteindre un niveau de sécurité approprié. Il en résulte qu'en cas de violation de l'obligation légale de sécurité, la charge de la preuve échoit à l'autorité de contrôle, au ministère public ou à la personne concernée qui devra démontrer que le débiteur n'a pas été suffisamment prudent ou diligent dans la mise en œuvre de moyens qui auraient été nécessaires pour l'éviter.

Cette affirmation mérite néanmoins d'être nuancée puisque l'exigence d'*accountability* a pour effet de renforcer cette obligation de moyens en imposant dorénavant au responsable du traitement d'être en mesure de démontrer l'efficacité des mesures *sur demande de l'autorité de contrôle*[147]. Cette obligation documentaire prend corps, d'une part, avec l'obligation de tenir un Registre[148], et, d'autre part, avec l'obligation du responsable du traitement de réaliser une AIPD pour les traitements « susceptibles d'engendrer un risque élevé »[149]. Ces documents sont une source non-négligeable d'informations utiles afin de jauger la prudence et la diligence dont doivent faire preuve les débiteurs de l'obligation de sécurité.

En effet, le Registre doit notamment contenir « dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles »[150]. Quant à l'AIPD, celle-ci doit, entre autres, impérativement étayer « les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer

---

145 CPVP, « note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 8.

146 « On se situe d'ailleurs pour l'essentiel dans le cadre d'obligations de moyens et ne seront nécessaires que les mesures dont l'effet de protection est dans un rapport adéquat avec les efforts qu'elles occasionnent ». Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 1990-1991, n° 1610/1, 6 mai 1991, p. 21.

147 Art. 58, § 1, a), du RGPD.

148 Art. 30 du RGPD. À noter que la CPVP recommande à *tous* les responsables de traitement et sous-traitants d'établir un Registre, CPVP, Recommandation n° 06/2017 relative au Registre des activités de traitements (article 30 du RGPD), 14 juin 2017, p. 7.

149 Art. 35 du RGPD.

150 Art. 30 du RGPD.

la protection des données à caractère personnel et à apporter la preuve du respect du [...] Règlement »[151]. Cependant, il convient de rappeler si que le Registre doit être mis à disposition de l'autorité de contrôle sur demande, il n'est par contre pas destiné aux personnes concernées ni au public en général. De même, il n'y a pas d'obligation légale de publier une AIPD. C'est le responsable du traitement qui décide lui-même de la publier ou non, quand bien même cette publication est encouragée par le Groupe 29[152]. Du point de vue des personnes concernées, l'obligation de sécurité de leurs débiteurs reste donc essentiellement une obligation de moyens même si les exigences documentaires susmentionnées contribueront solidement à l'évaluation des éventuels manquements par les autorités de contrôle, voire judiciaires[153].

19. En revanche, dans les relations entre le responsable du traitement et le sous-traitant, le principe de convention-loi ne s'oppose pas à ce que le contrat régissant leurs rapports contienne des obligations additionnelles de résultat en matière de sécurité informationnelle (par exemple en matière de contrôle des accès physiques et logiques, de journalisation, de techniques cryptographiques spécifiques, d'interdiction du BYOD, etc.). Dans cette éventualité, ces obligations de résultat permettront au responsable du traitement de mettre en jeu la responsabilité du sous-traitant par la simple constatation que le résultat n'a pas été atteint, sans avoir à prouver une quelconque faute. Le sous-traitant ne pourra alors se dégager de sa responsabilité que s'il parvient à prouver l'existence d'une cause étrangère comme la survenance d'un cas de force majeure, la faute du responsable du traitement ou le fait d'un tiers.

---

[151] Art. 35, § 7, d), du RGPD.

[152] « La publication peut accroître la confiance dans les opérations de traitement du responsable du traitement et donner des gages de transparence. Il est notamment de bonne pratique de publier une AIPD lorsque des citoyens sont affectés par l'opération de traitement. Tel peut en particulier être le cas lorsqu'une autorité publique réalise une AIPD. L'AIPD publiée n'a pas besoin d'inclure l'intégralité de l'analyse, notamment lorsque celle-ci pourrait donner des informations spécifiques relatives à des risques en matière de sécurité concernant le responsable du traitement ou divulguer des secrets d'affaires ou des informations commercialement sensibles. Dans pareille situation, la version publiée peut consister simplement en un résumé des principales constatations de l'AIPD, ou même uniquement en une déclaration selon laquelle une AIPD a été effectuée ». Groupe 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, WP 248, 4 avril 2017, p. 22.

[153] Art. 77 du RGPD.

CHAPITRE 4. L'identification de la nature, de la portée, du contexte et des finalités du traitement

SECTION 1. – Objet

20. L'obligation de sécurité étant essentiellement une obligation de moyens pour leurs débiteurs, il s'agit pour eux de déterminer la probabilité et la gravité du risque du traitement envisagé pour les droits et libertés de la personne concernée afin de prendre les mesures appropriées. À cet égard, le considérant n° 76 du règlement indique qu'un premier pas consiste à tenir compte « de la nature, de la portée, du contexte et des finalités du traitement »[154]. Par ailleurs, l'article 30 du RGPD prévoit les circonstances dans lesquelles les débiteurs de l'obligation de sécurité doivent tenir un Registre et précise le contenu « minimum » de celui-ci. Par souci de cohérence entre ces deux exigences, il nous semble judicieux d'aligner les contours de celles-ci puisqu'ainsi qu'illustré par le tableau ci-dessous, un Registre consciencieusement complété sera d'une aide précieuse afin d'identifier « la nature, la portée, le contexte et les finalités » des traitements envisagés.

[154] L'article 32, § 1, mentionne du RGPD les mêmes critères d'évaluation du risque. Parmi les éléments pertinents pour déterminer la nature, la portée, le contexte et les finalités des traitements, la CPVP cite « les catégories de personnes concernées, l'échelle du traitement de données, l'origine des données, la relation entre le responsable du traitement et les personnes concernées, les éventuelles conséquences pour les personnes concernées et le degré de facilité avec lequel on peut identifier ces dernières ». Voy. CPVP, Recommandation n° 01/2018, *op. cit.*, p. 17.

ID RT[155] : ID DPO[156]	Dénomination du traitement			
Traitement[157]	**Nature ?**	**Portée ?**	**Contexte ?**	**Finalité ?**
Informations légalement requises dans le Registre	- Une description des catégories de personnes concernées ; - Une description des catégories de données personnelles traitées, au regard de chacune des finalités identifiées.	- Les catégories de destinataires (internes et externes – y compris les sous-traitants) qui ont un accès autorisé aux données, y compris les destinataires dans des pays tiers à l'Union européenne ou des organisations internationales, au regard de chacune des finalités identifiées ; - Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et […] les documents attestant de l'existence de garanties appropriées.	- Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ; - Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, § 1, du RGPD.	La finalité de chaque traitement énoncée clairement et avec précision.

[155] Art. 30, § 1, a), du RGPD. La CPVP a développé des outils pour guider les responsables de traitement dans le remplissage de leur(s) déclaration(s) préalables de traitement dans une notice explicative disponible sur son site Internet. Cette notice explicative peut-être utile pour aider les débiteurs de l'obligation de sécurité à tenir leur Registre. En ce qui concerne particulièrement les informations requises pour l'identification du responsable du traitement, du sous-traitant, nous renvoyons le lecteur aux pages 4 à 7 dudit document. CPVP, Notice explicative de la déclaration préalable de traitement, juillet 2007, disponible à l'adresse https://www.privacycommission.be/sites/privacycommission/files/documents/notice_decl_ordinaire_0.pdf

[156] Art. 30, § 1, a), et 37, § 7, du RGPD

[157] La notion de traitement est très large et englobe, comme défini à l'article 4, 2), du RGPD, toute une série d'opérations allant de la collecte, à la consultation, la diffusion,

Recommandations d'informations supplémentaires à insérer dans le Registre	- Échelle du traitement : volume (par catégorie) de données traitées et nombre (par catégorie) de personnes concernées ; - Les supports des données.		- Taille du débiteur de l'obligation de sécurité ; - Statut du débiteur de l'obligation de sécurité ; - Mention qu'il s'agit de traitements qui imposent de procéder à une protection AIPD ; - Le relevé documenté de toutes les violations de données à caractère personnel tel que requis par l'article 33, § 5.	- Le fondement de licéité des données ; - L'origine des données ; - Moyens du traitement.

Figure 3 – Recommandations d'informations devant contenir le Registre

SECTION 2. – Le registre des activités de traitement : un outil méthodologique

21. Afin de « forcer » les débiteurs de l'obligation de sécurité à étayer méthodologiquement la nature, la portée, le contexte et les finalités des traitements envisagés, l'article 30 du RGPD met à charge des responsables de traitement et des sous-traitants l'obligation de tenir un Registre conçu comme un des outils du principe d'*accountability*. Cette nouvelle obligation – aussi dénommée « obligation de documentation interne » au cours de la négociation du RGPD[158] – poursuit un objectif comparable à la notification préalable des traitements prévue sous le régime de

l'interconnexion ou encore à l'enregistrement, à la destruction, à la pseudonymisation ou à l'anonymisation. Dans le cadre du registre, la CPVP utilise la notion de « finalité liée ». Voy. CPVP, *Notice explicative de la déclaration préalable de traitement notice*, *op. cit.*, p. 11.

[158] CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 4.

la Directive[159]. Toutefois, en Belgique notamment, la déclaration auprès de la CPVP était souvent perçue comme une pure et ennuyeuse formalité administrative et par conséquent souvent non exécutée[160]. Partant, le RGPD supprime cette obligation de déclaration préalable et opte pour la tenue d'un Registre exclusivement interne, non destiné aux personnes concernées ni au public en général[161], mais qui doit être fourni à l'autorité de contrôle à première demande[162]. Le lien avec l'autorité de contrôle n'est donc pas rompu ; il s'inscrit désormais dans la logique d'*accountability* du RGPD et dans l'évolution des missions des autorités de protection des données vers davantage de contrôle a posteriori que d'interventions en amont des traitements[163]. Etant donné que la « cartographie » des traitements de données opérés par les débiteurs de l'obligation de sécurité est essentielle à ceux-ci pour disposer d'une vue d'ensemble des traitements *non-occasionnels*[164] *à sécuriser, la CPVP recommande à tous* les responsables de traitement et sous-traitants[165] d'établir ce Registre[166], qu'ils soient ou non tenus de le maintenir aux termes du RGPD[167].

---

[159] Art. 18 de la Directive.

[160] « Le même constat a été fait dans les autres pays de l'Union européenne où une obligation de déclaration préalable de traitement similaire est en place en application de la directive 95/46/CE ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 9.

[161] À la différence du Registre – outil interne – la notification préalable entendait également porter un certain nombre d'informations aux traitements à la connaissance des personnes concernées via le registre public (et en ligne) dans lequel elles sont intégrées.

[162] Art. 30, § 4, du RGPD. De plus, l'article 31 du RGPD exige du responsable de traitement et du sous-traitant une pleine coopération avec l'autorité de contrôle.

[163] CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 9.

[164] « Comment définir le caractère non occasionnel d'un traitement ? « Occasionnal », terme anglais (langue de travail et de négociation du RGPD) doit être compris comme « occurring or appearing at irregular or infrequent intervals ; occurring now and then », soit un traitement qui est tel par occasion, par hasard, fortuit par opposition à habituel. Ne sont par exemple pas des traitements occasionnels, les traitements de données liés à la gestion de la clientèle, à la gestion du personnel (ressources humaines) ou encore à la gestion des fournisseurs ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 6.

[165] Il convient de noter que les éléments que doit contenir ce Registre au regard des traitements réalisés en qualité de sous-traitant sont un peu différents de ceux réalisés en qualité de responsable de traitement. En effet, en ce qui concerne les sous-traitants, seuls les éléments directement pertinents pour l'activité de sous-traitance, listés à l'article 30(2) du RGPD, doivent être repris dans le Registre. Pour un aperçu plus précis des éléments que doit contenir le Registre d'un sous-traitant, voy. CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 16.

[166] « Toutefois, s'agissant des PME, et compte tenu de la portée très limitée de l'exception à l'obligation d'établir un Registre, la CPVP n'est pas opposée à ce que le Registre se limite aux traitements non occasionnels. Les traitements occasionnels ne devraient donc pas y figurer ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 7.

[167] L'obligation de tenir un Registre comporte une exception pour les « entreprises ou organisations comptant moins de 250 employés ». Cette exception est néanmoins toute relative puisque les entreprises visées devront tout de même tenir un Registre lorsqu'elles

Ce Registre, écrit, et disponible en version électronique, doit contenir les informations suivantes :

- le nom et les coordonnées du responsable de traitement et le cas échéant du responsable conjoint[168] du traitement, du représentant du responsable de traitement et du délégué à la protection des données ;
- la finalité de chaque traitement énoncée clairement et avec précision[169] ;
- une description des catégories de personnes concernées[170] et des catégories de données personnelles traitées[171], au regard de chacune des finalités identifiées ;

---

se trouvent dans l'une des 4 hypothèses suivantes : le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et libertés des personnes concernées ; le traitement qu'elles effectuent n'est pas occasionnel ; le traitement qu'elles effectuent porte sur des données sensibles ; le traitement qu'elles effectuent porte sur des données judiciaires.

[168] Voy. l'article 26 du RGPD sur les responsables conjoints. En cas de responsables conjoints, chacun des responsables conjoints doit, dans le Registre qui est le sien, faire état des traitements opérés dès lors que l'article 30, § 1, impose que les traitements réalisés sous leur responsabilité figurent dans le Registre.

[169] De manière générale, il faut veiller à ce que les finalités du traitement soient *décrites avec la précision nécessaire*. Il faut éviter un renvoi à des finalités générales, décrites au sens large (comme par ex. « améliorer l'expérience d'utilisateur », « sécurité IT », « analyse »). La description de la finalité doit donner à celui qui consulte le Registre – en ce compris l'autorité de contrôle – une idée claire des traitements de données opérés.

[170] On pense évidemment aux employés, aux clients, aux fournisseurs, aux prestataires externes. De plus, le Groupe 29 estime qu'il s'agit également d'identifier les catégories de personnes considérées comme étant vulnérables « en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits ». Peuvent être considérés comme des personnes concernées vulnérables, « les enfants (qui peuvent être vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données), les employés, les segments les plus vulnérables de la population nécessitant une protection particulière (personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.) et, en tout état de cause, toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié ». Groupe 29, WP 248, *op. cit.*, p. 12.

[171] L'identification des catégories de données traitées revient bien sûr à procéder à une description des données à caractère personnel qui font l'objet du traitement. Par ailleurs, il est recommandé d'opérer une classification desdites données. Il s'agit, tout d'abord, d'énumérer les données à caractère personnel traitées selon le traitement envisagé. De manière *non-exhaustive*, citons par exemple les données d'identification, les caractéristiques personnelles, les caractéristiques du logement, les études et les formation, la profession et l'emploi, les particularités financières, les habitudes de vie, les données physiques, les données psychiques, la composition de ménage, les loisirs et intérêts, les habitudes de consommation, les enregistrements de sons ou d'images, les affiliations à des organisations caritatives ou bénévoles, clubs, associations, unions, organisations, groupements, réseaux sociaux, etc. Il convient également d'identifier les catégories de données à caractère personnel qui sont, par

- les catégories de destinataires[172] auxquels les données ont été ou seront communiquées[173], y compris les destinataires dans des pays tiers à l'Union européenne ou des organisations internationales, au regard de chacune des finalités identifiées ;
- le cas échéant les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas de transferts visés à l'article 49(1) alinéa 2, les documents attestant de l'existence de garanties appropriées, et ce, au regard de chacune des finalités identifiées[174] ;

---

nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, et qui, par conséquent, méritent une protection spécifique car elles peuvent « engendrer des risques importants pour ces libertés et droits ». Il s'agit des catégories particulières de données à caractère personnel (en vertu de l'article 9) ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions (en vertu de l'article 10). Enfin, le Groupe 29 suggère qu'il y a lieu d'énumérer les catégories de « données à caractère hautement personnel » en considérant « qu'au-delà des dispositions du RGPD, certaines catégories de données peuvent être considérées comme augmentant le risque possible pour les droits et libertés des personnes. Ces données à caractère personnel sont considérées comme sensibles (au sens commun du terme) dans la mesure où elles sont liées à des activités domestiques et privées (communications électroniques dont la confidentialité doit être protégée, par exemple), dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte met en cause la liberté de circulation, par exemple) ou dans la mesure où leur violation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple) ». Groupe 29, WP 248, *op. cit.*, p. 11.

[172] La notion de destinataire est définie à l'article 4, 9), du RGPD comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ». Sont donc visés, tant d'éventuels destinataires internes (tels les employés) qu'externes (tels les sous-traitants ou des tiers), y compris les destinataires dans des pays tiers à l'Union européenne ou des organisations internationales, au regard de chacune des finalités identifiées. De plus, l'obligation de tenir un Registre des traitements étant une obligation dynamique, « le responsable du traitement et le sous-traitant veilleront à le tenir à jour en ajoutant par exemple tout nouveau destinataire qu'ils n'auraient pas pu envisager lors de la rédaction originelle du Registre (ex : inspection fiscale, nouveau partenaire commercial…) ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 14.

[173] Dans sa notice explicative de déclaration préalable, la CPVP met à disposition un tableau qui reprend les principales catégories de destinataires auxquels le responsable du traitement communique éventuellement des données à caractère personnel. CPVP, *Notice explicative de la déclaration préalable de traitement*, *op. cit.*, p. 27.

[174] Doivent également répertoriés, les documents attestant de l'existence de garanties appropriées, et ce, au regard de chacune des finalités identifiées. En effet, « l'article 49, § 2 du RGPD exige qu'en l'absence de décision d'adéquation, en l'absence de garanties appropriées telles que les règles d'entreprises contraignantes (BCR), en l'absence de situations dans lesquelles les exceptions telles que le consentement ou encore le contrat par exemple trouvent à s'appliquer, des garanties appropriées entourent le transfert de données

- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données[175] ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, § 1, du RGPD.

Conçu comme un outil de l'*accountability*, relevons également que rien ne s'oppose à ce que le Registre contienne davantage d'informations que celles explicitement énumérées à l'article 30 du RGPD. Dans la mesure du possible, le Registre contiendra donc utilement des informations additionnelles telles que :

- la mention du fondement de licéité du traitement[176] ;
- la mention qu'il s'agit de traitements qui imposent de procéder à une analyse d'impact relative à la protection des données[177] ;

---

nécessaires aux fins des intérêts légitimes impérieux poursuivi par le responsable de traitement lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée. Il s'agit d'une hypothèse (intérêt légitime impérieux) dans laquelle des flux de données vers un pays tiers sont autorisés qui est tout à fait subsidiaire, de dernier recours. Cette disposition ne doit être utilisée comme fondement au transfert qu'à titre tout à fait exceptionnel et de strictes garanties doivent entourer ces transferts, garanties prévues par exemple dans un contrat à répertorier dans le Registre ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 14.

[175] Cet élément d'information rejoint le principe selon lequel les données ne peuvent être conservées sous une forme permettant l'identification des personnes que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. « Par durée de conservation, il ne faut pas nécessairement comprendre une durée en jours, mois, années, soit une évaluation quantitative. La durée de conservation peut également faire référence à des paramètres tels que le temps nécessaire à la réalisation de la finalité concrète poursuivie ainsi qu'à la gestion du contentieux éventuel y relatif, l'expiration d'un délai de prescription, une durée d'archivage légal après la fin du traitement, etc. ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 15.

[176] La mention du fondement de licéité du traitement est utile à mentionner dans le Registre étant donné qu'en en cas de consentement, le responsable doit pouvoir démontrer qu'il a obtenu celui-ci (art. 7, § 1, du RGPD). De manière analogue, en cas de traitement fondé sur l'intérêt légitime, le responsable du traitement doit préciser quel est cet intérêt légitime (art. 13, § 1, d), et 14, § 2, b), du RGPD). Notons également qu'en ce qui concerne le traitement des données sur le lieu de travail, le Groupe 29 a encore récemment rappelé que « le consentement est très peu susceptible de constituer une base juridique pour le traitement des données sur le lieu de travail, à moins que les employés ne puissent refuser le traitement sans conséquences défavorables ; l'exécution d'un contrat et des intérêts légitimes peuvent parfois être invoqués, à condition que le traitement soit strictement nécessaire à des fins légitimes et respecte les principes de proportionnalité et de subsidiarité. De plus les employés devraient recevoir des informations concrètes au sujet de la surveillance qui est menée et tout transfert international de données relatives aux employés ne devrait avoir lieu que si un niveau de protection adéquat est garanti ». Groupe 29, WP 249, *op. cit.*, p. 3.

[177] Voy. la section 6 du chapitre 2 de la présente contribution.

- le relevé documenté de toutes les violations de données à caractère personnel tel que requis par l'article 33(5) du RGPD afin de permettre à l'autorité de contrôle de vérifier le respect de l'article 33 relatif à la notification des violations de données[178].
- la taille[179] et le statut[180] du débiteur de l'obligation de sécurité ;
- l'échelle du traitement : volume (par catégorie) de données traitées et nombre (par catégorie) de personnes concernées[181] ;
- l'origine des données[182] ;

[178] « Que cette information soit disponible dans le Registre visé par l'article 30 du RGPD ou ailleurs importe peu du moment que l'information est disponible pour l'autorité de contrôle ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 17.

[179] De manière générale, le RGPD ne prévoit pas d'exception en fonction de la taille des responsables de traitement et sous-traitants, pour les Petites et Moyennes Entreprises par exemple (ci-après PME) : « l'approche par le risque reflétée dans une série d'obligations du RGPD s'accommode mal de ce type d'exceptions. Il serait à tout le moins incohérent de considérer qu'en toutes hypothèses, la taille d'un responsable de traitement ou d'un sous-traitant signifie une absence de risque ou un risque faible pour les droits et libertés des individus ». CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 4. Néanmoins, le Groupe 29 considère que « les mesures attendues […] devraient être modulables et prendre en compte, entre autres critères, le type de la société (sa taille, son statut de société à responsabilité limitée) ». Groupe 29, WP 168, *op. cit.*, p. 23. De même, dans son vade-mecum à destination des PME, la CPVP estime que « l'approche basée sur les risques signifie que les obligations qui découlent du RGPD varient en fonction du risque lié à l'activité de traitement. Le RGPD crée donc une marge pour parvenir à une solution sur mesure pour chaque PME ». CPVP, « RGPD vade-mecum pour les PME : Un guide pour préparer les petites et moyennes entreprises (PME) au règlement général sur la protection des données », janvier 2018, p. 5. En ce qui concerne plus particulièrement les mesures de sécurité que devraient prendre en compte les PME, l'ENISA a publié des « Guidelines for SMEs on the security of personal data processing » afin d'aider celles-ci dans leur approche. ENISA, « Guidelines for SMEs on the security of personal data processing », décembre 2016. Ces invitations de « prise en compte » ne permettent cependant pas de dérogations nouvelles. CPVP, *Recommandation n° 06/2017*, *op. cit.*, p. 5.

[180] Dans sa notice explicative, la CPVP estimait également que le statut du débiteur de l'obligation de sécurité pouvait donner une idée du contexte dans lequel les données sont traitées. CPVP, *Notice explicative de la déclaration préalable de traitement*, *op. cit., p.* 8.

[181] Évaluer l'échelle du traitement est également utile pour déterminer la nature de celui-ci étant donné que le traitement de données traitées à grande échelle constitue un des critères pouvant entraîner un risque inhérent élevé et une éventuelle obligation de conduire une AIPD.

[182] Lorsqu'un traitement a lieu pour une fin autre que celle pour laquelle les données ont été collectées initialement et n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, l'article 6, § 4, b), requiert que l'analyse de la compatibilité de cette finalité ultérieure tienne compte du « contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ». Le Groupe 29 va dans le même sens en affirmant qu'il s'agit d'analyser « *the specific context in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situation would expect his or her data to be used for based on the context of the collection* ». Voy. Groupe 29, Opinion 03/2013 on purpose limitation, WP 203, 2 avril 2013, p. 24.

- les supports des données[183] ;
- les moyens du traitement[184].

Enfin, le Registre étant un outil vivant, amené à évoluer en fonction du développement des activités de l'entreprise, de l'autorité ou de l'organisme concerné, il doit constamment être tenu à jour. Enfin, il est utile de mentionner que compte tenu de la variété des situations, il n'existe pas de canevas-type unique du Registre. Toutefois, des modèles de Registres ont déjà été mis à disposition, par exemple, par la CPVP[185] et par la CNIL[186].

[183] Selon la CNIL, il est également utile de recenser les supports sur lesquels reposent les traitements de données à caractère personnel, notamment : les matériels (ex : serveurs, ordinateurs portables, disques durs) ; les logiciels (ex : système d'exploitation, logiciel métier) ; les canaux de communication (ex : fibre optique, Wi-Fi, Internet) ; les supports papier (ex : document imprimé, photocopie). CNIL, « La sécurité des données personnelles », *op. cit.*, p. 3.

[184] La CPVP recommande de décrire de manière suffisamment détaillée et claire les moyens techniques et opérationnels du traitement. Une visualisation de ces moyens peut contribuer à favoriser une approche systématique pour déterminer précisément la finalité de celui-ci. CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 17.

[185] Le modèle de Registre de la CPVP est disponible à l'adresse https://www.privacycommission.be/fr/node/20442.

[186] Le modèle de Registre de la CNIL est disponible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx.

CHAPITRE 5. Une obligation de sécurité axée autour des risques pour les personnes physiques

22. Ainsi que le souligne le Groupe 29, l'approche fondée sur les risques (« *risk-based approach* ») n'est pas un concept nouveau[187], puisqu'il était déjà bien connu sous l'empire de la Directive[188]. Cependant, le RGPD prête davantage d'attention à cette approche puisqu'elle n'est plus seulement explicitement le pivot de l'obligation de sécurité, mais également au centre de l'exigence d'*accountability*. En effet, les deux types de contraintes – étroitement liées entre elles pour les raisons précédemment invoquées – imposent

---

[187] Groupe 29, WP 163, *op. cit.*, p. 2.

[188] « *The so-called "risk-based approach" is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20). The legal regime applicable to the processing of special categories of data (Article 8) can also be considered as the application of a risk-based approach : strengthened obligations result from processing which is considered risky for the persons concerned* ». Groupe 29, WP 218, *op. cit.*, p. 2.

à leurs débiteurs *de pouvoir démontrer* leur prise en compte des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques[189]. Selon le Groupe 29, l'approche du RGPD fondée sur les risques a donc pour but de promouvoir une « approche évolutive et proportionnelle »[190] sans toutefois dispenser du respect des principes fondamentaux. Ainsi, les principes en matière de qualité des données et les droits des personnes concernées doivent toujours être respectés, quels que soient les risques qu'un traitement déterminé engendre[191]. Toutefois, l'obligation de sécurité étant essentiellement une obligation de moyens, cette approche implique que les débiteurs de l'obligation de sécurité doivent prendre davantage de mesures pour des traitements présentant un « risque élevé »[192] que pour des traitements à risque faible[193].

SECTION 1. – La notion

23. Le considérant n° 4 du RGPD rappelle que « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité »[194]. Il est donc logique que l'obligation de sécurité soit principalement axée autour de la notion de « risques pour les droits et libertés des personnes physiques »[195]. Contrairement à la gestion de risques dans d'autres domaines – comme par exemple la sécurité de l'information qui est généralement orientée sur les intérêts et les finalités de l'organisation elle-même – le RGPD se place sous l'angle du risque pour les droits et libertés des personnes concernées afin de déterminer le niveau de sécurité approprié. Quant à la nature des droits à prendre en compte, le Groupe 29 indique que la référence aux « droits et libertés » des personnes concernées ne renvoie pas uniquement au droit à la vie privée ou au droit à la protection des données, « mais s'entend également, le cas échéant, pour d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion »[196]. Un

189 Art. 24, § 1, et 32, § 1, du RGPD.
190 En anglais : « *a scalable and proportionate approach to compliance* ». Groupe 29, WP 218, *op. cit.*, p. 2.
191 *Ibid.*
192 La notion de « risque élevé » est analysée au § 1 de la section 2, du chapitre 6.
193 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 6.
194 Considérant n° 4 du RGPD.
195 Considérant n° 75 du RGPD.
196 Groupe 29, WP 248, *op. cit.*, p. 7.

« risque » est donc une possibilité que survienne une conséquence négative pour lesdits droits et libertés des personnes physiques, résultant d'un traitement accidentel ou illicite de données à caractère personnel[197].

SECTION 2. – Les sources des risques pour les personnes physiques

24. L'article 5, § 1, f), du règlement exige que les données soient protégées *y compris* contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle. À cet égard, le règlement élargit quelque peu l'objet de la protection requise par l'article 17, § 1, de la Directive, notamment par l'ajout de la locution prépositive « y compris ». Cette précaution de non-exhaustivité semble suggérer que la protection requise astreint à prévenir tout traitement effectué en violation du règlement[198]. De manière similaire, dans le cadre de l'évaluation des risques pour la sécurité des données, « il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, *tels que* la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite […] »[199]. Ainsi que nous l'avons mentionné plus haut, « selon les besoins », il peut donc être également souhaitable de prendre en compte les risques résultant d'une indisponibilité temporaire non voulue du traitement, que celle-ci soit accidentelle (par exemple une coupure de courant) ou illicite (par exemple suite à un DDoS).

En ce qui concerne le vocabulaire utilisé, la notion de « traitements non-autorisés » couvre les circonstances dans lesquelles des données sont traitées « sans droit » par des tiers, des destinataires ou par des personnes placées sous l'autorité directe du responsable du traitement ou du sous-traitant. Les termes « de manière accidentelle ou illicite » renvoient, quant à eux, aux traitements « non autorisés » réalisés respectivement de manière purement accidentelle ou de manière intentionnelle.

La problématique des traitements non-autorisés des données informatiques n'est pas neuve. En février 1990, les tribunaux belges eurent déjà à traiter du cas d'un Bourgmestre ayant permis l'accès au registre national à des personnes n'appartenant pas au personnel communal

197 *Ibid.*
198 Considérant n° 83.
199 Art. 32, § 2, et considérant n° 83 du RGPD.

autorisé[200]. La même année, deux personnes pirataient le serveur informatique du premier ministre de l'époque, Wilfried Martens, à l'aide d'un mot de passe détourné[201], ce qui n'avait pas manqué de mettre « la criminalité informatique dans tous ses états »[202]. Plus récemment, partout à travers le monde, des entreprises ont fait l'objet d'attaques dirigées vers les données : Myspace, Ebay, LinkedIn, Dropbox mais également, Ashley Madison, ou encore Yahoo à qui 500 millions de profils d'utilisateurs ont été volés. Criminalité et sécurité informatique sont ainsi les deux versants de la même médaille. Comme l'indique le Groupe 29, « l'intégration de la protection des données dans les cultures des organisations aidera les autorités chargées de la protection des données à mener à bien leurs missions de contrôle et de lutte contre la criminalité [...], ce qui aura pour effet d'accroître l'efficacité des mesures de protection de la vie privée »[203].

Conscient de l'enjeu, dès 2001, le Conseil de l'Europe adopta la Convention de Budapest laquelle prohibe notamment l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système, les abus de dispositifs, la falsification informatique et la fraude informatique. Chaque Partie doit adopter dans son droit interne les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales ces actes commis intentionnellement et sans droit. En Belgique, le Code pénal réprime ainsi notamment le faux informatique[204], la fraude informatique[205], le hacking – tant externe[206] qu'interne[207] –, le

[200] Corr. Charleroi, 10e ch., 1er février 1990, *J.L.M.B.*, 1990, p. 1147.

[201] Corr. Bruxelles, 8 novembre 1990, *J.T.*, 1990, p. 11 et Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340.

[202] T. Verbiest et I. Dervaux, « La criminalité informatique dans tous ses états », *R.D.C.* 2002, liv. 8, 607-613.

[203] Groupe 29, WP 168, *op. cit.*, p. 21.

[204] Art. 210*bis* C. pén. Le faux informatique requiert une altération de la vérité par l'introduction, la modification ou l'effacement de données qui sont stockées, traitées ou transmises par un système informatique ou par la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique avec une *intention frauduleuse ou le dessein de nuire*. Comme pour le faux en écritures de droit commun, il est requis que les données manipulées aient une portée juridique. À ce sujet, voy. O. Leroux, « Criminalité informatique », in *Les infractions contre les biens*, Bruxelles, Larcier, 2008, p. 388. Pour une étude approfondie de cette incrimination, voy. O. Leroux, « Le faux informatique », *J.T.*, 2004, pp. 509 et s.

[205] L'article 504*quater* du Code pénal incrimine celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique.

[206] L'article 550*bis*, § 1er, du Code pénal sanctionne celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient.

[207] L'article 550*bis*, § 2, du Code pénal vise celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique.

sabotage[208] ainsi que les actes non-autorisés de prise de connaissance des communications électroniques[209] Selon l'infraction envisagée, l'élément moral requis est un dol général ou spécial[210].

Cela étant dit, tout détournement de finalité résultant d'un traitement « non autorisé » ne sera pas forcément qualifié d'infraction de criminalité informatique. Ainsi, dans un arrêt de janvier 2017, la Cour de cassation a considéré qu'une employée d'une ville belge qui disposait d'un accès illimité à l'ensemble du système informatique à des fins d'assistance technique, de maintenance et de dépannage ne commettait pas un hacking interne en accédant à certaines données à des fins totalement différentes et étrangères à ses missions, dans la mesure où la personne disposait d'un pouvoir d'accès aux données[211]. Un tel agissement doit, par contre, être considéré comme une violation du principe édicté à l'article 29 du RGPD selon lequel « le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre ».

SECTION 3. – Un risque à géométrie variable

25. Pour ce qui est de l'évaluation des risques pour les droits et libertés des personnes physiques, l'article 32 du RGPD précise explicitement que leur « degré de probabilité et de gravité varie ». De même, le Groupe 29 définit le « risque » comme « un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité »[212]. L'on comprend donc que le risque doit être analysé au regard de deux variables : sa probabilité, d'une part, et sa gravité de l'autre[213].

---

[208] L'article 550*ter* du Code pénal réprime celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique.

[209] Voy. not. art. 314*bis* et 259*bis* C. pén.

[210] Pour une analyse de ces infractions, lire O. Leroux, « Section 1. - Criminalité informatique spécifique », in *Les infractions*, vol. 1, Bruxelles, Larcier, 2016, pp. 448-508.

[211] Cass., 24 janvier 2017, R.G. n° P. 16.0048.N, *T. Strafr.*, 2017/3, pp. 206-207.

[212] Groupe 29, WP 248, *op. cit.*, p. 7.

[213] Voy. égal. ISO, « Risk management – Vocabulary », ISO Guide 73 :2009 (« un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance »).

§ 1. La probabilité du risque

26. En ce qui concerne l'analyse de la première variable, il faut admettre que le texte du RGPD n'est pas des plus clairs. En effet, évaluer la probabilité d'un risque revient à l'idée de statistiquement analyser la récurrence potentielle d'un événement possible qui n'est peut-être encore jamais intervenu. Néanmoins, dans son « Handbook on Security of Personal Data Processing »[214], rédigé en collaboration avec les APD hellénique et italienne, l'ENISA propose, entre autres, une méthodologie destinée à évaluer la probabilité de la matérialisation d'un risque. Selon cette approche, les quatre dimensions principales suivantes doivent faire l'objet d'un examen scrupuleux afin de déterminer la probabilité d'un incident :

A. Les ressources techniques et de réseau (hardware et software) ;

B. Les processus et procédures régissant le traitement ;

C. Les différents destinataires externes et internes impliqués dans le traitement ;

D. Le secteur concerné ainsi que l'échelle du traitement.

Les tableaux ci-dessous reproduisent les points qui, selon l'ENISA, devraient entrer en considération lors de l'évaluation de la probabilité de la matérialisation d'un risque[215].

A. NETWORK AND TECHNICAL RESOURCES		
1.	**Is any part of the processing of personal data performed through the internet ?**	When the processing of personal data is performed fully or partially through the open Internet, possible threats from external online attackers increase (e.g. Denial of Service, SQL injection, Man-in-the-Middle attacks), especially when the service is available (and, thus, traceable/known) to all internet users.
2.	**Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users) ?**	When access to an internal data processing system is provided through the internet, the likelihood of external threats increases (e.g. due to external online attackers). At the same time the likelihood of (accidental or intentional) misuse of data by the users also increases (e.g. accidental disclosure of personal data when working in public spaces). Special attention should be given to cases where remote management/administration of the IT system is allowed.

[214] ENISA, « Handbook on Security of Personal Data Processing », décembre 2017, disponible à l'adresse

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport.

[215] *Ibid.*, pp. 12 à 14.

3.	**Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service ?**	Connection to external IT systems may introduce additional threats due to the threats (and potential security flaws) that are inherent to those systems. The same applies also to internal systems, taking into account that, if not appropriately configured, such connections may allow access (to the personal data) to more persons within the organization (which are not in principle authorized for such access).
4.	**Can unauthorized individuals easily access the data processing environment ?**	Although focus has been put on electronic systems and services, the physical environment (relevant to these systems and services) is an important aspect that, if not adequately safeguarded, can seriously compromise security (e.g. by allowing unauthorized parties to gain physical access to the IT equipment and network components or failing to provide protection of the computer room in the event of a physical disaster).
5.	**Is the personal data processing system designed, implemented or maintained without following relevant best practices ?**	Poorly designed, implemented and/or maintained hardware and software components can pose serious risks to information security. To this end, good or best practices accumulate the experience of prior events and can be regarded as practical guidelines of how to avoid exposure and achieve certain levels of resilience

B. PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA		
6.	**Are the roles and responsibilities with regard to personal data processing vague or not clearly defined ?**	When roles and responsibilities are not clearly defined, access (and further processing) of personal data may be uncontrolled, resulting to unauthorized use of resources and compromising the overall security of the system.
7.	**Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined ?**	When acceptable use of resources is not clearly mandated, security threats might arise due to misunderstanding or intentional misuse of the system. The clear definition of policies for network, system and physical resources can reduce potential risks.
8.	**Are the employees allowed to bring and use their own devices to connect to the personal data processing system ?**	Employees using their personal devices within the organization could increase the risk of data leakage or unauthorized access to the information system. Moreover, as devices are not centrally controlled, they may introduce additional bugs or viruses into the system.

9.	**Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organization ?**	Processing of personal data outside the premises of the organization can offer a lot of flexibility, but at the same time introduces additional risks, both related to the transmission of information through possibly insecure network channels (e.g. open Wi-Fi networks), as well as unauthorised use of this information.
10.	**Can personal data processing activities be carried out without log files being created ?**	The lack of appropriate logging and monitoring mechanisms can increase intentional or accidental abuse of processes/procedures and resources, resulting to the subsequent abuse of personal data.

C. PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA		
11.	**Is the processing of personal data performed by a non-defined number of employees ?**	When access (and further processing) of personal data is open to a large number of employees, the possibilities of abuse due to human factor increase. Clearly defining who really needs to access the data and limiting access only to those persons can contribute to the security of personal data.
12.	**Is any part of the data processing operation performed by a contractor/third party (data processor) ?**	When the processing is performed by external contractors, the organization may lose partially the control over these data. Moreover, additional security threats may be introduced due to the threats that are inherent to these contractors. It is important for the organization to select contractors that can offer a high level of security and to clearly define what part of the processing is assigned to them, maintaining as much as possible a high level of control.
13.	**Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated ?**	When employees are not clearly informed about their obligations, threats from accidental misuse (e.g. disclosure or destruction) of data many significantly increase.
14.	**Is personnel involved in the processing of personal data unfamiliar with information security matters ?**	When employees are not aware of the need of applying security measures, they can accidentally pose further threats to the system. Training can greatly contribute to making employees aware both of their data protection obligations, as well as the application of specific security measures.

15.	**Do persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data ?**	Many personal data breaches occur due to the lack of physical protection measures, such as locks and secure destruction systems. Paper based files are usually part of the input or the output of an information system, can contain personal data and should also be protected from unauthorized disclosure and re-use.

D. BUSINESS SECTOR AND SCALE OF PROCESSING		
16.	**Do you consider your business sector as being prone to cyberattacks ?**	When security attacks have already taken place in a specific business sector, there is an indication that the organization would probably need to take additional measures to avoid a similar event.
17.	**Has your organization suffered any cyberattack or other type of security breach over the last two years ?**	If the organization has already been attacked or there are indications that this might have been the case, additional measures need to be taken to prevent similar events in the future.
18.	**Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year ?**	Security bugs/vulnerabilities can be exploited to perform attacks (cyber or physical) to systems and services. Security bulletins containing important information regarding security vulnerabilities that could affect the aforementioned systems and services should be considered.
19.	**Does a processing operation concern a large volume of individuals and/or personal data ?**	The type and volume of personal data (scale) can make the processing operation attractive to attackers (due to the inherent value of these data).
20.	**Are there any security best practices specific to your business sector that have not been adequately followed ?**	Sector specific security measures are usually adjusted to the needs (and risks) of the particular sector. Lack of compliance with relevant best practices might be an indicator of poor security management.

Figure 4 – L'évaluation de la probabilité d'un risque selon l'ENISA

§ 2. La gravité du risque

27. Quant à l'analyse de la gravité d'un risque, le considérant n° 75 du RGPD donne plusieurs exemples non limitatifs de *conséquences négatives* pour les droits et libertés des personnes physiques, à savoir « la discrimination, un vol ou une usurpation d'identité, des pertes financières, une

atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel, la suppression non autorisée de la pseudonymisation, la situation où des personnes concernées ne peuvent pas exercer leurs droits et libertés ou sont empêchées d'exercer le contrôle sur leurs données à caractère personnel et, enfin, tout autre dommage économique ou social important ». La CPVP cite également comme exemples de conséquences négatives potentielles pour les droits et libertés des personnes concernées « la perte d'une opportunité, l'atteinte portée à la tranquillité ou au bien-être, la stigmatisation ou le stéréotypage, le refus ou la limitation d'accès à des lieux ou événements qui sont d'habitude accessibles au public, le traitement déloyal (par exemple fixation des prix différenciée), la manipulation (par exemple l'exploitation d'émotions), l'adaptation de comportement (par exemple autocensure) ou encore l'atteinte portée à l'intégrité physique ou morale »[216].

Le risque étant par nature un événement dont la survenance n'est pas certaine mais qui peut potentiellement entraîner des « dommages physiques, matériels ou un préjudice moral »[217] pour les personnes concernées, sa gravité est évidemment liée aux dommages potentiels qu'il peut engendrer. Il va de soi que le dommage physique repose, par définition, sur le principe de l'inviolabilité du corps humain. Quant au dommage matériel, celui-ci se définit comme le résultat d'une atteinte aux biens d'une personne, ou encore à ses possibilités d'en acquérir, de les accroître ou de les gérer[218]. Enfin, le « dommage moral », dans son acception la plus large, comprend « les souffrances morales (sentiment de diminution et d'inquiétude face à l'avenir), les souffrances physiques (appelées également quantum doloris ou pretium doloris), le préjudice psychologique, le préjudice d'agrément, le préjudice esthétique, le préjudice sexuel ou encore le préjudice d'affection, etc. »[219]. Ainsi que le souligne Y. Poullet, les trois types de dommages cités ci-dessus peuvent bien entendu apparaître séparément ou simultanément à cause de la réalisation d'un risque. L'auteur ajoute « *a priori*, le dommage immatériel paraît le plus bénin, et le dommage "physique" le plus grave, mais il ne nous paraît pas souhaitable d'établir une véritable gradation de ces dommages. En effet, une "échelle" des dommages est toujours sujette à controverses et risque, en outre, de conduire à diminuer la prévention des dommages jugés moins graves. Or, cela ne semble pas entrer dans les intentions du législateur européen, qui vise à protéger les "libertés et droits fondamentaux des personnes", indépendamment du type de dommage éventuellement subi »[220].

---

216 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 21.

217 Considérant n° 75 du RGPD.

218 Y. Poullet, « La sécurité informatique, entre technique et droit », *op. cit.*, p. 20.

219 C. trav. Mons (10e ch.), 16 décembre 2015, R.G. n° 2015/AM/313.

220 Y. Poullet, « La sécurité informatique, entre technique et droit », *op. cit.*, p. 20.

CHAPITRE 6. L'évaluation des risques

SECTION 1. – Objet

28. Le considérant n° 83 du RGPD indique qu'afin « de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents […] ». Afin d'appliquer ce précepte, une distinction préalable entre le risque « inhérent » et le risque « résiduel » doit être opérée. Selon la CPVP, « le risque "inhérent" renvoie à la probabilité qu'un impact négatif se produise lorsqu'aucune mesure de protection n'est prise. Le risque "résiduel" renvoie au contraire à la probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent) »[221].

Ayant clarifié ces notions, l'analyse des risques inhérents engloberait « l'ensemble du processus : d'identification des risques, d'analyse des risques et d'évaluation des risques »[222]. D'après l'autorité nationale, « l'identification des risques reviendrait à examiner, reconnaître et décrire les risques ; l'analyse du risque au processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque. Enfin, l'évaluation du risque viserait le processus de comparaison des résultats de l'analyse du risque avec les critères de risque préétablis afin de déterminer si le risque (et/ou son importance) est (sont) acceptable(s) ou tolérable(s) »[223].

Ainsi qu'illustré dans les précédentes sections, la gravité et/ou la probabilité d'un risque peut fortement varier en fonction de la nature, de la portée, du contexte, des finalités du traitement ainsi que des sources du risque. Par conséquent, le RGPD impose tant au responsable du traitement qu'au sous-traitant d'évaluer les risques inhérents afin de pouvoir déterminer le caractère « approprié » des mesures techniques et organisationnelles mises en place pour atténuer ces risques inhérents et de parvenir à un risque résiduel acceptable ou tolérable. Enfin, tous les traitements de données à caractère personnel ne donnent pas lieu aux mêmes risques inhérents : certains risques inhérents pouvant être qualifiés d'élevés et d'autres non.

---

221 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 20.

222 ISO, « Risk management – Vocabulary », ISO Guide 73 :2009. Lors de l'identification des risques, le responsable du traitement doit faire preuve de la prudence nécessaire et anticiper les risques potentiels, même si la nature du risque n'est pas connue à l'avance. L'évaluation du niveau de risque n'a en effet lieu que lors de l'analyse ultérieure des risques identifiés.

223 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 19.

SECTION 2. – Les traitements susceptibles d'engendrer un risque inhérent élevé

§ 1. Notion de risque élevé

29. Le considérant n° 84 du règlement dispose qu'afin « de mieux garantir le respect du présent règlement lorsque les opérations de traitement *sont susceptibles d'engendrer un risque élevé* pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque ».

La notion de « risque élevé » n'est pas définie en détail dans le RGPD[224]. Consciente du fait que des organisations différentes utilisent des échelles et des méthodes différentes lorsqu'elles procèdent à une évaluation des risques, la CPVP estime « qu'il est dès lors possible que l'interprétation de ces valeurs diffère selon l'échelle de risque et la méthode utilisées »[225]. Toutefois, de manière générale, la notion de « risque élevé » renverrait aux traitements de données qui « sont ou pourront être *susceptibles* d'avoir des *incidences négatives sensibles* pour les libertés et droits fondamentaux des personnes physiques. L'expression "susceptible de" ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées : la probabilité qu'elles soient sensiblement affectées suffit pour répondre à ce critère. Une "conséquence négative sensible" signifie que, dans le cas où le risque inhérent se produirait, la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux »[226].

La notion de « risque élevé » bourgeonnait déjà dans la Directive. En effet, l'article 20, § 1, de celle-ci prévoyait que les États membres devaient préciser les traitements susceptibles de présenter des « risques particuliers » au regard des droits et libertés des personnes concernées et veiller à ce que ces traitements soient examinés *avant* leur mise en œuvre. Le considérant n° 53 précisait que ces « risques particuliers »

[224] La notion de « risque élevé » au sens du RGPD ne correspond toutefois pas nécessairement à la notion de « risque élevé » telle qu'on la retrouve dans d'autres modèles de gestion des risques puisque le RGPD vise à protéger les risques pour les droits et libertés des personnes physiques.

[225] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 8.

[226] *Ibid.*

pouvaient découler « du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle ». Pour de tels traitements à « risque particulier » les États membres devaient prévoir un examen préalable à leur mise en œuvre[227].

§ 2. L'obligation d'effectuer une AIPD en cas de risque élevé

30. Sous le régime du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, une AIPD doit être effectuée « avant le traitement »[228]. Cette exigence est cohérente avec les principes de protection des données dès la conception et de protection des données par défaut[229]. De plus, dans le cas où la conduite d'une AIPD n'est pas considérée comme étant nécessaire du fait qu'un risque inhérent n'est pas identifié comme étant « élevé », il faudra pourtant *logiquement* procéder à une analyse de risques afin de motiver et de documenter la raison pour laquelle le responsable du traitement est parvenu à cette conclusion[230].

Cela étant dit, le paragraphe 3 de l'article 35 précise qu'une AIPD est, *en particulier,* requise dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire[231] ;
- le traitement à grande échelle de catégories particulières de données visées à l'article 9, § 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou

[227] Considérant n° 54 de la Directive.

[228] Art. 35, §§ 1 et 10, et considérants n^os^ 90 et 93 du RGPD. À moins qu'il s'agisse d'un traitement déjà existant ayant préalablement fait l'objet d'un examen par l'autorité de contrôle, auquel cas l'AIPD sera effectuée avant toute mise en œuvre de modifications significatives.

[229] Art. 25 et considérant n° 78 du RGPD.

[230] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 11.

[231] L'article 35, § 3, a), du RGPD évoque des « décisions » produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. Il est important de faire remarquer qu'il n'est pas requis qu'il s'agisse d'une prise de décision « entièrement automatisée » au sens de l'article 22 du RGPD. Dès lors, l'article 35, § 3, a), du RGPD s'applique aussi lorsque la prise de décision en question ne se base pas exclusivement sur un traitement automatisé.

- la surveillance systématique[232] à grande échelle d'une zone accessible au public[233].

Comme le laissent entendre les mots « en particulier » dans la phrase introductive de l'article 35, § 3, du RGPD, il s'agit là d'une liste *non exhaustive*. Même si elles ne figurent pas dans cette énumération, d'autres opérations de traitement peuvent néanmoins présenter un risque inhérent aussi élevé[234].

§ 3. Les critères du Groupe 29 pour identifier un risque inhérent élevé

31. Pour déterminer s'il est ou non probable qu'un traitement envisagé puisse donner lieu à un risque inhérent élevé, les lignes directrices élaborées par le Groupe 29[235] sont particulièrement importantes puisqu'elles identifient neuf critères qui doivent être pris en considération dans l'analyse déterminant si un traitement envisagé est ou non susceptible d'engendrer un risque inhérent élevé pour les droits et libertés des personnes physiques[236]. Ces critères sont les suivants :

a) Évaluation ou notation, y compris les activités de profilage et de prédiction, portant notamment sur des « aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements »[237].

---

[232] Le RGPD ne définit pas ce que l'on entend par la notion de « systématique ». D'après le Groupe 29, cette notion doit être interprétée selon une ou plusieurs des manières qui suivent : une chose qui se déroule selon un système ; qui est préparée, organisée ou méthodique ; qui se déroule dans le cadre d'un plan général de collecte de données ; qui est réalisée dans le cadre d'une stratégie.

[233] Une « zone accessible au public » est un lieu, quel qu'il soit, ouvert à tout un chacun, tel qu'une place, un centre commercial, une rue, un marché, une gare ou encore une bibliothèque publique, par exemple. CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 13.

[234] Groupe 29, WP 248, *op. cit.*, p. 10.

[235] Les lignes directrices du Groupe 29 « s'efforcent de promouvoir la mise en place : d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD est obligatoire (article 35, paragraphe 4) ; d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD n'est pas nécessaire (article 35, paragraphe 5) ; de critères communs concernant la méthodologie à suivre pour la réalisation d'une AIPD (article 35, paragraphe 5) ; de critères communs pour la détermination des cas dans lesquels l'autorité de contrôle doit être consultée (article 36, paragraphe 1) ; de recommandations basées sur l'expérience acquise dans les États membres de l'UE, dans la mesure du possible ».

[236] Groupe 29, WP 248, *op. cit.*, pp. 10-13.

[237] Considérants n^os^ 71 et 91 du RGPD. Le Groupe 29 donne à titre d'exemples, « le cas d'un établissement financier passant ses clients au crible d'une base de données de cote de crédit ou d'une base de données dédiée à la lutte contre le blanchiment de capitaux et le

b) Prise de décision automatisée avec effet juridique ou effet similaire significatif : ce critère comprend des traitements axés sur la prise de décisions relatives aux personnes concernées « produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire »[238]. Le traitement pourrait, par exemple, entraîner l'exclusion ou une discrimination. Les traitements n'ayant que peu ou pas d'effet sur les personnes ne répondent pas à ce critère particulier[239].

c) Surveillance systématique : ce critère comporte des traitements utilisés pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux et par la surveillance systématique d'une zone accessible au public. Il s'agit d'un critère étant donné que la collecte des données à caractère personnel est susceptible d'intervenir dans des circonstances telles que les personnes concernées ne savent pas qui collecte leurs données et de quelle façon elles seront utilisées. En outre, il peut être impossible pour les personnes de se soustraire à un tel traitement dans l'espace public (ou accessible au public) considéré[240].

d) Données sensibles ou données à caractère hautement personnel : ce critère comporte les catégories particulières de données à caractère personnel visées à l'article 9 (informations concernant les opinions politiques des personnes, par exemple) ainsi que des données à caractère personnel

---

financement du terrorisme (LBC/FT) ou « antifraude », celui d'une société de biotechnologie proposant des tests génétiques directement aux consommateurs afin d'évaluer et de prédire les risques de maladie/de problèmes de santé, ou encore celui d'une entreprise analysant les usages ou la navigation sur son site Web pour créer des profils comportementaux ou marketing ». Groupe 29, WP 248, *op. cit.*, p. 10.

[238] Art. 35, § 3, a), du RGPD.

[239] Voy. égal. art. 35, § 3, a), du RGPD. Ce critère est présent lorsque le traitement peut par exemple entraîner l'exclusion ou une discrimination de personnes physiques. Un traitement n'ayant que peu ou pas d'effet sur les personnes physiques ne répond pas à ce critère particulier. Des explications complémentaires concernant ces notions sont fournies dans les lignes directrices du Groupe 29 relatives au profilage. Groupe 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev.01, 3 octobre 2017 et révisé le 6 février 2018.

[240] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 9. « Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées : exploitation d'un réseau de télécommunications ; fourniture de services de télécommunications ; reciblage par courrier électronique ; activités de marketing fondées sur les données ; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent) ; géolocalisation, par exemple, par des applications mobiles ; programmes de fidélité ; publicité comportementale ; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables ; systèmes de télévision en circuit fermé ; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc. ».

relatives aux condamnations pénales ou aux infractions visées à l'article 10. Il comporte également les données à caractère personnel qui sont considérées de manière générale comme sensibles dans la mesure où elles sont liées à des activités domestiques et privées (communications électroniques dont la confidentialité doit être protégée, par exemple), dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte peut influencer la liberté de mouvement, par exemple) ou dans la mesure où leur divulgation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple)[241].

e) Traitement de données à caractère personnel à grande échelle, compte tenu :

- du nombre de personnes concernées (soit en valeur absolue, soit en proportion de la population considérée) ;
- du volume de données et/ou de l'éventail des différents éléments de données traitées ;
- de la durée ou de la permanence de l'activité de traitement de données ;
- de l'étendue géographique de l'activité de traitement[242].

f) Croisement ou combinaison d'ensembles de données, par exemple issus de deux opérations de traitement de données, ou plus, effectuées à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée[243].

g) Données concernant des personnes vulnérables, comme par exemple les enfants, les travailleurs, les personnes souffrant de maladie mentale, les demandeurs d'asile, les personnes âgées, les patients et autres segments les plus vulnérables de la population nécessitant une protection particulière[244]. Le traitement de ce type de données est un critère en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les

[241] Voy. égal. considérant n° 45 du RGPD. À titre d'exemple, citons les dossiers médicaux que peut conserver un hôpital général ou encore les informations sur des auteurs d'infractions que peut détenir un enquêteur privé. CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 10.

[242] Le considérant n° 91 du RGPD précise que l'obligation de conduire une analyse d'impact préalable ne s'applique pas aux traitements de données à caractère personnel de patients ou de clients effectués par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, le traitement ne peut être considéré comme étant à grande échelle.

[243] Voy. égal. considérants n^{os} 75 et 91 du RGPD. Voy. aussi Groupe 29, Lignes directrices concernant les délégués à la protection des données, *op. cit.*, p. 9.

[244] Voy. égal. considérant n° 75 du RGPD.

premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer aisément au traitement de leurs données ou d'exercer leurs droits.

h) Utilisation ou application innovante de nouvelles solutions technologiques ou organisationnelles, comme l'utilisation combinée de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc. Il s'agit d'un critère parce que l'utilisation de la technologie en question peut impliquer de nouvelles formes de collecte et d'utilisation des données, présentant potentiellement un risque élevé pour les droits et libertés des personnes physiques[245].

i) Lorsque les personnes concernées ne peuvent pas exercer un droit ou bénéficier d'un service ou d'un contrat. Cela comprend les opérations visant à autoriser, modifier ou refuser l'accès des personnes concernées à un service ou la possibilité de ces personnes de conclure un contrat.

§ 4. Prise en compte des critères du Groupe 29 dans la qualification du risque

32. Dans la plupart des cas, le responsable du traitement pourrait considérer qu'un traitement satisfaisant à deux des neufs critères identifiés par le Groupe 29 nécessite une AIPD[246]. D'une manière générale, le Groupe estime que plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD, quelles que soient les mesures que le responsable du traitement envisage d'adopter. Néanmoins, dans certains cas, le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD. À l'inverse, une opération de traitement peut correspondre à l'un des cas susmentionnés et être néanmoins considérée par le responsable du traitement comme non « susceptible d'engendrer un risque élevé ». Dans pareil cas, il convient que le responsable du traitement explique et documente les motifs de sa décision de ne pas procéder à une AIPD en incluant/rapportant par ailleurs l'opinion à cet égard du délégué à la protection des données. Dans ses lignes directrices, le Groupe cite des exemples qui illustrent la

[245] En outre, il est clairement précisé dans le RGPD que l'utilisation d'une nouvelle technologie peut impliquer la nécessité de réaliser une analyse d'impact relative à la protection des données. Voy. art. 35, § 1, et considérants n^{os} 89 et 91 du RGPD. « Le fait de déterminer si une technologie doit être considérée ou non comme étant « nouvelle » doit se faire « en conformité avec l'état des connaissances technologiques » ». CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 11.

[246] Groupe 29, WP 248, *op. cit.*, p. 13.

façon dont il convient d'utiliser les critères pour déterminer si une opération de traitement considérée nécessite une AIPD[247].

De plus, une AIPD peut être nécessaire à la suite d'une évolution des risques découlant des opérations de traitement, par exemple en raison du recours à une nouvelle technologie ou de l'utilisation des données à caractère personnel à des fins différentes. Les opérations de traitement peuvent évoluer rapidement et de nouvelles vulnérabilités peuvent apparaître. Par conséquent, il convient de noter que la révision d'une AIPD est non seulement utile dans un souci d'amélioration continue, mais également essentielle pour maintenir le niveau de protection des données dans un environnement qui change au fil du temps. Une AIPD peut également devenir nécessaire du fait d'une évolution du contexte organisationnel ou sociétal de l'activité de traitement, par exemple s'il s'avère que les effets de certaines décisions automatisées se sont accrus ou que de nouvelles catégories de personnes concernées apparaissent vulnérables à la discrimination. Dans chacun de ces exemples, le facteur en cause peut entraîner une évolution des risques découlant de l'activité de traitement concernée. Inversement, certaines évolutions peuvent aussi réduire les risques. Prenons par exemple le cas d'une opération de traitement ayant évolué de telle sorte que les prises de décisions ne sont plus automatisées ou celui d'une activité de surveillance ayant perdu son caractère systématique. Dans ce cas, le réexamen des risques peut montrer qu'une AIPD n'est plus nécessaire[248].

§ 5. Projet de liste de la CPVP de traitements soumis à l'AIPD

33. L'article 35, § 4, du RGPD oblige chaque autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD est requise[249] et à communiquer ensuite cette liste au Comité européen de la protection des données (ci-après « CEPD »)[250].

---

[247] Groupe 29, WP 248, *op. cit.*, pp. 13 à 14.

[248] Groupe 29, WP 248, *op. cit.*, p. 16.

[249] La compétence de dresser une liste des types de traitements pour lesquels une AIPD est obligatoire au sens de l'article 35, § 4, du RGPD n'incombe pas à la CPVP mais à l'Autorité de protection des données, l'instance qui succédera de plein droit à la CPVP à partir du 25 mai 2018. Dès lors, la liste ci-après ne sera juridiquement contraignante que si elle est arrêtée par l'Autorité de protection des données, le cas échéant après application du mécanisme de contrôle de la cohérence visé à l'article 63 du RGPD. De plus, la CPVP souligne que l'existence d'une liste des opérations de traitement pour lesquelles une AIPD est requise ne porte en rien préjudice à l'obligation générale du responsable du traitement de procéder à une bonne appréciation du risque et à une bonne gestion des risques. La simple circonstance qu'un traitement de données envisagé ne corresponde pas avec un des types de traitement repris dans la liste (par exemple parce qu'une des caractéristiques n'est pas présente) ne signifie donc pas qu'il y aurait pour ce traitement une dispense de l'obligation de réaliser une AIPD conformément à l'article 35, § 1, du RGPD.

[250] Art. 35, § 6, du RGPD. Lorsque cette liste comprend des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement

Par conséquent, outre les cas prévus à l'article 35, § 3, du RGPD et compte tenu de l'exception prévue par l'article 35, § 10, du RGPD, une AIPD sera toujours requise selon la CPVP[251] :

a) lorsque le traitement utilise des données biométriques en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public ;

b) lorsque des données à caractère personnel sont collectées auprès de tiers afin d'être prises ensuite en considération dans le cadre de la décision de refuser ou de cesser un contrat de service déterminé avec une personne physique ;

c) lorsque le traitement concerne des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD qui sont (ré) utilisées pour une (des) finalité(s) autre(s) que celle(s) pour laquelle (lesquelles) elles ont été collectées, sauf lorsque le traitement se fonde sur le consentement de la personne concernée ou s'il est nécessaire pour répondre à une obligation légale à laquelle le responsable du traitement est soumis[252] ;

d) lorsque le traitement est réalisé à l'aide d'un implant et qu'une violation de données à caractère personnel pourrait compromettre la santé physique de la personne concernée ;

e) en cas de traitement à grande échelle de données à caractère personnel de personnes physiques vulnérables, notamment les enfants, pour une (des) finalité(s) autre(s) que celle(s) pour laquelle (lesquelles) elles ont été collectées ;

f) lorsque des données sont collectées à grande échelle auprès de tiers afin d'analyser ou de prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;

g) lorsque des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD ou des données de nature très

---

dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union, il faut appliquer préalablement à l'établissement de la liste le mécanisme de contrôle visé à l'article 63.

[251] Le responsable du traitement qui envisage un des types de traitements précités est obligé de réaliser une AIPD avant de procéder au traitement. Cela ne signifie toutefois pas nécessairement qu'une consultation préalable doit également avoir lieu. Si le risque peut être suffisamment limité à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable n'est requise.

[252] Il s'agit ici d'un traitement de catégories particulières de données pour une finalité autre que celle pour laquelle les données ont été collectées et qui n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, tel que visé par l'article 6, § 4, du RGPD.

personnelle (comme des données sur la pauvreté, le chômage, l'implication de l'aide à la jeunesse ou le travail social, des données sur les activités domestiques et privées, des données de localisation) sont échangées systématiquement entre plusieurs responsables du traitement ;

h) lorsqu'il est question d'un traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs qui envoient des données via Internet ou via un autre moyen (applications de "l'Internet des objets", comme les télévisions intelligentes, les appareils ménagers intelligents, les jouets connectés, les smart cities, les compteurs d'énergie intelligents, etc.) et que ce traitement sert à analyser ou prédire la situation économique, la santé, les préférences ou centres d'intérêt ; personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;

i) lorsqu'il est question d'un traitement à grande échelle et/ou systématique de données de téléphonie, d'Internet ou d'autres données de communication, de métadonnées ou de données de localisation de personnes physiques ou permettant de mener à des personnes physiques (par exemple le wifi-tracking ou le traitement de données de localisation de voyageurs dans les transports publics) lorsque le traitement n'est pas strictement nécessaire pour un service demandé par la personne concernée ;

j) lorsqu'il est question de traitements de données à caractère personnel à grande échelle où le comportement de personnes physiques est observé, collecté, établi ou influencé, y compris à des fins publicitaires, et ce de manière systématique via un traitement automatisé[253].

SECTION 3. – Les traitements non soumis à l'obligation d'AIPD

34. À titre introductif, rappelons qu'une analyse des risques inhérents doit être réalisée qu'il y'ait ou non une obligation (ou une forte recommandation de procéder à une AIPD). En effet, le fait de ne pas réaliser une AIPD ne dispense pas les responsables de traitements et les sous-traitants de leur obligation générale de prendre des mesures pour gérer de manière appropriée tous les risques pour les droits et libertés des personnes concernées conformément à l'article 32 du RGPD.

[253] La CPVP cite, « par exemple le comportement de visionnage, d'écoute, de navigation, de clic, physique ou d'achat ». CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 44.

§ 1. Les critères énumérés par le Groupe 29

35. Le Groupe 29 considère qu'une AIPD n'est pas nécessaire dans les cas suivants :

- lorsque le traitement n'est pas « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[254] ;
- lorsque le traitement est très similaire en termes de nature, de portée, de contexte et de finalités à un autre traitement qui a fait l'objet d'une AIPD. Dans un tel cas, les résultats de l'AIPD réalisée pour le traitement similaire peuvent être utilisés[255] ;
- lorsque le traitement a fait l'objet d'un examen mené par une autorité de contrôle avant mai 2018 dans des conditions spécifiques qui n'ont pas changé[256] ;
- lorsque le traitement a pour fondement de licéité le respect d'une obligation légale[257] ou l'exécution d'une mission d'intérêt public[258] et qu'il a une base juridique dans le droit de l'Union ou dans le droit de l'État membre, que ce droit règlemente l'opération de traitement spécifique et qu'une AIPD a déjà été réalisée dans le cadre de l'établissement de la base juridique en question[259], à moins qu'un État membre n'estime

---

[254] Art. 35, § 1, du RGPD.

[255] Art. 35, § 1, du RGPD selon lequel « une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

[256] Aucune AIPD n'est nécessaire pour les opérations de traitement qui ont fait l'objet d'un examen par une autorité de contrôle ou par le détaché à la protection des données, conformément à l'article 20 de la directive 95/46/CE, et dont la mise en œuvre n'a pas changé depuis le contrôle préalable. En effet, selon le considérant n° 171, « les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées ». À l'inverse, ceci signifie que tout traitement de données dont les conditions de mise en œuvre (portée, finalités, données à caractère personnel collectées, identité des responsables du traitement ou des destinataires des données, durée de conservation des données, mesures techniques et organisationnelles, etc.) ont changé depuis l'examen préalable effectué par l'autorité de contrôle ou le détaché à la protection des données et sont susceptibles d'engendrer un risque élevé doit faire l'objet d'une AIPD.

[257] Art. 6, § 1, c), du RGPD.

[258] Art. 6, § 1, e), du RGPD.

[259] Art. 35, § 10, du RGPD. Dans le cas d'une AIPD réalisée au stade de l'élaboration de la législation conférant une base juridique au traitement, un réexamen pourra être nécessaire avant le lancement des opérations, la législation adoptée étant susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il est possible que les détails techniques disponibles en ce qui concerne le traitement effectif soient insuffisants au moment de l'adoption de la législation, même si une AIPD a été effectuée. Dans de tels cas, il pourra s'avérer nécessaire d'effectuer une AIPD spécifique avant d'exécuter les activités de traitement proprement dites.

qu'il est nécessaire de procéder à une telle analyse avant les activités de traitement ;

- lorsque le traitement figure dans la liste facultative (établie par l'autorité de contrôle) des opérations de traitement qui ne requièrent pas d'AIPD[260]. Cette liste peut recenser les activités de traitement conformes aux conditions fixées par l'autorité en question, en particulier par l'intermédiaire de lignes directrices, de décisions ou autorisations spécifiques, de règles de conformité, etc. Dans pareil cas et sous réserve d'une réévaluation par l'autorité de contrôle compétente, il n'est pas nécessaire d'effectuer une AIPD, à la condition exclusive, toutefois, que le traitement relève strictement du champ d'application de la procédure pertinente indiquée dans la liste et continue de satisfaire pleinement à toutes les exigences applicables du RGPD.

Enfin, le CEPD peut également publier des lignes directrices relatives aux opérations de traitement considérées comme étant peu susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et indiquer les mesures qui peuvent suffire dans de tels cas pour faire face à un tel risque[261].

§ 2. Projet de liste de la CPVP de traitements non soumis à l'AIPD

36. Ainsi que nous l'avons mentionné, l'article 35, § 5, du RGPD autorise l'autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD n'est pas requise[262].

Par conséquent, dans l'annexe 3 de ses recommandations[263], la CPVP estime que pour les types de traitement suivants, une AIPD n'est pas requise :

a) Obligation légale : les traitements réalisés par des entités privées qui sont nécessaires pour répondre à une obligation légale qui leur incombe, moyennant une définition par la loi des finalités du traitement, des

[260] Art. 35, § 5, du RGPD.

[261] Considérant n° 77 du RGPD.

[262] La CPVP souligne que la liste susmentionnée ne porte en rien préjudice à l'obligation générale du responsable du traitement de procéder à une bonne appréciation du risque et à une bonne gestion des risques, conformément à l'article 24, § 1, du RGPD. Cette obligation générale d'appréciation du risque et de gestion des risques s'applique sans préjudice de l'existence d'une liste de traitements spéciaux pour lesquels une AIPD n'est pas requise en tant que telle. Enfin, la Commission attire encore l'attention sur le fait que ces listes sont évolutives et peuvent être adaptées s'il s'avère qu'elles n'atteignent pas leur objectif.

[263] CPVP, *Recommandation n° 01/2018*, *op. cit.*, annexe 3.

catégories de données à caractère personnel traitées et des garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;

b) Administration des salaires : les traitements de données à caractère personnel qui concernent uniquement des données qui sont nécessaires à l'administration des salaires de personnes en service ou actives pour le compte du responsable du traitement lorsque les données sont exclusivement utilisées pour cette administration des salaires, sont uniquement communiquées aux destinataires qui sont autorisés à cet effet et ne sont pas conservées plus longtemps que le temps nécessaire aux finalités du traitement ;

c) Administration du personnel : les traitements de données à caractère personnel qui concernent exclusivement l'administration du personnel en service ou actif pour le compte du responsable du traitement, dans la mesure où ce traitement ne porte pas sur des données relatives à la santé de la personne concernée, ni sur des catégories particulières de données au sens de l'article 9 du RGPD, ni sur des condamnations pénales et des infractions au sens de l'article 10 du RGPD ou sur des données ayant pour but une évaluation de la personne concernée et où les données à caractère personnel traitées ne sont pas conservées plus longtemps que le temps nécessaire à l'administration du personnel et uniquement dans le cadre de l'application d'une disposition légale ou réglementaire ou sont communiquées si nécessaire à des tiers pour la réalisation des finalités du traitement ;

d) Comptabilité : les traitements de données à caractère personnel qui concernent exclusivement la comptabilité du responsable du traitement lorsque les données sont exclusivement utilisées pour cette comptabilité, lorsque le traitement concerne uniquement les personnes dont les données sont nécessaires pour la comptabilité et lorsque les données à caractère personnel ne sont pas conservées plus longtemps que nécessaire à la réalisation des finalités du traitement et que les données à caractère personnel traitées sont uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire ou lorsque la communication est nécessaire pour la comptabilité ;

e) Administration des actionnaires et des associés : les traitements de données à caractère personnel qui concernent exclusivement l'administration des actionnaires et associés lorsque le traitement porte uniquement sur des données nécessaires à cette administration, lorsque ces données concernent uniquement des personnes dont les données sont nécessaires à cette administration, lorsque les données sont communiquées à des tiers uniquement dans le cadre de l'application d'une disposition légale ou réglementaire et que les données à caractère personnel ne sont pas conservées plus longtemps que le temps nécessaire à la réalisation des finalités du traitement ;

f) Les traitements des fondations et ASBL : les traitements de données à caractère personnel effectués par une fondation, association ou toute autre institution sans but lucratif dans le cadre de ses activités habituelles, pour autant que le traitement porte uniquement sur des données à caractère personnel relatives à ses propres membres, relatives aux personnes avec lesquelles le responsable du traitement entretient des contacts réguliers et relatives aux bénéficiaires de la fondation, association ou institution et qu'aucune personne ne soit enregistrée sur la base de données obtenues de tiers et que les données à caractère personnel traitées ne soient pas conservées plus longtemps que le temps nécessaire à l'administration des membres, des personnes de contact et des bénéficiaires et soient uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire ;

g) Le contrôle d'accès des visiteurs : les traitements de données à caractère personnel qui concernent exclusivement l'enregistrement de visiteurs dans le cadre d'un contrôle d'accès lorsque les données traitées restent limitées au nom et à l'adresse professionnelle du visiteur, à l'identification de son employeur, à l'identification du véhicule du visiteur, au nom, à la section et à la fonction de la personne visitée et au moment de la visite et où les données à caractère personnel traitées peuvent exclusivement être utilisées pour le contrôle d'accès et ne pas être conservées plus longtemps que le temps nécessaire à cette finalité ;

h) La gestion des élèves ou étudiants : les traitements de données à caractère personnel effectués par des établissements d'enseignement en vue de la gestion de leurs relations avec leurs élèves ou étudiants dans le cadre de leurs missions d'enseignement, dans la mesure où le traitement ne porte que sur des données à caractère personnel relatives à des élèves ou étudiants potentiels, actuels et anciens de l'établissement d'enseignement en question et qu'aucune personne ne soit enregistrée sur la base de données obtenues de tiers et que ces données soient uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire et ne soient pas conservées plus longtemps que le temps nécessaire à la gestion de la relation avec l'élève ou l'étudiant ;

i) Gestion de la clientèle ou fournisseurs : les traitements de données à caractère personnel qui concernent exclusivement la gestion de la clientèle ou des fournisseurs du responsable du traitement, pour autant que le traitement concerne uniquement des clients ou fournisseurs existants et anciens du responsable du traitement et que le traitement ne concerne pas des catégories particulières de données au sens de l'article 9 du RGPD, ni des condamnations pénales et des infractions visées à l'article 10 du RGPD et qu'en ce qui concerne l'administration de la clientèle, aucune donnée provenant de tiers soit enregistrée et que les données à caractère

personnel traitées ne soient pas conservées pour une durée excédant celle nécessaire à la gestion normale de l'entreprise du responsable du traitement et ces données ne peuvent être transmises à des tiers que dans le cadre de l'application d'une disposition légale ou réglementaire ou pour la gestion normale de l'entreprise.

CHAPITRE 7. L'analyse d'impact relative à la protection des données

SECTION 1. – Objet

37. Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face. Les AIPD sont un outil important au regard du principe d'*accountability*, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des exigences du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au règlement. Autrement dit, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve[264].

L'AIPD doit être lancée le plus tôt possible dans le cycle de conception du traitement, même si certaines opérations de traitement sont encore inconnues. La mise à jour de l'AIPD tout au long du projet assurera la prise en compte des questions liées à la protection des données et de la vie privée et encouragera la création de solutions favorisant la conformité. Il peut également être nécessaire de répéter les différentes étapes de l'évaluation au fur et à mesure de l'avancée du processus de développement étant donné que le choix de certaines mesures techniques ou organisationnelles peut modifier la gravité ou la probabilité des risques associés au traitement[265]. Le fait que l'AIPD puisse devoir être actualisée après le lancement effectif du traitement n'est pas une raison valable pour la différer

[264] Notre section relative à l'analyse d'impact est fortement basée sur Groupe 29, WP 248, *op. cit.* et CPVP, *Recommandation n° 01/2018*, *op. cit.*

[265] Groupe 29, WP 248, *op. cit.*, p. 17.

ou pour ne pas l'effectuer. Une telle analyse est un processus continu, en particulier lorsque l'opération de traitement est dynamique et soumise à de constants changements[266]. De plus, l'obligation d'effectuer une AIPD s'applique aux opérations de traitement *existantes* susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et pour lesquelles les risques associés ont évolué, compte tenu de la nature, de la portée, du contexte et des finalités du traitement[267].

En outre, le simple fait que les conditions déclenchant l'obligation d'effectuer une AIPD – décrites plus haut – ne soient pas remplies ne restreint toutefois pas l'exigence générale faite aux débiteurs de l'obligation de sécurité d'évaluer les risques afin de mettre en œuvre des mesures appropriées. Enfin, cela signifie que les responsables du traitement sont tenus d'évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[268]. En cas de doute quant à la nécessité d'effectuer une AIPD, dans la mesure où les AIPD sont un outil important pour les responsables du traitement aux fins du respect de la législation sur la protection des données, le Groupe 29 recommande d'en effectuer une malgré tout[269].

SECTION 2. – Étendue de l'AIPD

38. Une AIPD peut concerner une opération de traitement de données unique. Cependant, l'article 35, § 1, dispose qu'« une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ». Le considérant n° 92 ajoute qu'« il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée ».

Une seule et même AIPD peut donc être utilisée pour évaluer plusieurs opérations de traitement similaires en termes de nature, de portée, de

266 *Ibid.*
267 *Ibid.*, p. 16.
268 *Ibid.*, p. 7.
269 *Ibid.*, p. 9.

contexte, de finalités et de risques. En effet, « les AIPD visent à assurer l'étude systématique des nouvelles situations susceptibles d'entraîner des risques élevés pour les droits et libertés des personnes physiques, et il n'est pas nécessaire de procéder à une AIPD dans les cas (à savoir des opérations de traitement effectuées dans un contexte spécifique et à des fins spécifiques) qui ont déjà été étudiés. Tel peut être le cas lorsque des technologies similaires sont utilisées pour collecter le même type de données pour les mêmes finalités. Par exemple, un groupe d'autorités municipales mettant chacune en place un système similaire de surveillance par CCTV pourrait se contenter d'une AIPD unique couvrant le traitement envisagé par chacun de ces responsables distincts ; un opérateur ferroviaire (un seul responsable du traitement) pourrait quant à lui couvrir la vidéosurveillance de l'ensemble de ses gares au moyen d'une seule et même AIPD. Ceci peut également valoir pour des opérations de traitement similaires mises en œuvre par différents responsables du traitement. Dans pareils cas, il y a lieu qu'une AIPD de référence soit partagée ou rendue publiquement accessible, les mesures décrites dans l'AIPD doivent être mises en œuvre et une justification de la réalisation d'une AIPD unique doit être fournie. Lorsque l'opération de traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives. Il convient que leur AIPD détermine quelle partie est responsable des différentes mesures destinées à faire face aux risques et à protéger les droits et libertés des personnes concernées, et que chaque responsable du traitement exprime ses besoins et partage les informations utiles en veillant à ne pas compromettre de secrets (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles, par ex.) et à ne pas divulguer de vulnérabilités publiquement »[270]. Une AIPD peut également être utile « pour évaluer l'impact sur la protection des données d'un produit technologique, par exemple un matériel ou un logiciel, lorsque celui-ci est susceptible d'être utilisé par divers responsables du traitement pour réaliser différentes opérations de traitement. Bien entendu, le responsable du traitement déployant le produit reste tenu d'effectuer sa propre AIPD pour ce qui concerne sa mise en œuvre spécifique, mais il peut s'appuyer pour cela sur une AIPD élaborée par le fournisseur du produit, le cas échéant. Prenons l'exemple de la relation entre fabricants de compteurs intelligents et entreprises de services publics. Il conviendrait que chaque fournisseur ou sous-traitant partage les informations utiles en s'assurant de ne compromettre aucun secret ni de menacer la sécurité en divulguant des vulnérabilités »[271].

[270] *Ibid.*
[271] *Ibid.*

SECTION 3. – Rôles des différents acteurs lors de l'exécution de l'AIPD

§ 1. Le responsable du traitement

39. L'obligation de procéder à une AIPD incombe en premier lieu au responsable du traitement. Il est celui qui en endosse la responsabilité finale et doit rendre compte si l'AIPD n'est pas (ou pas correctement) réalisée lorsque celle-ci est bel et bien obligatoire en vertu de l'article 35 du RGPD. L'AIPD peut être réalisée par quelqu'un d'autre, à l'intérieur ou à l'extérieur de l'organisation, mais le responsable du traitement reste responsable en dernier ressort de cette tâche[272].

La CPVP estime indispensable que le responsable du traitement veille à ce que les bonnes personnes au sein de l'entreprise soient impliquées dans le processus d'évaluation des risques[273]. Il est recommandé de documenter expressément la tâche et le rôle de chacune de ces personnes lors de la réalisation (de parties) d'une AIPD[274] en tenant compte de la politique, des processus et des règles internes[275].

§ 2. Le sous-traitant

Le sous-traitant doit, en fonction de la nature du traitement, assister le responsable du traitement dans l'exécution d'une AIPD. Dans les précédentes versions du projet du RGPD, il était même explicitement prévu que l'obligation de procéder à une AIPD en tant que telle reposerait également

---

[272] *Ibid.*, p. 18.

[273] Selon la CPVP, « afin d'éviter que le processus d'évaluation des risques soit ramené à un pur exercice écrit, ceux qui sont les mieux placés pour contribuer à une évaluation des risques de qualité doivent être impliqués en temps opportun dans le processus d'identification, d'évaluation et de gestion des risques. La Commission pense ici en premier lieu non seulement au délégué à la protection des données et/ou au conseiller en sécurité, mais aussi aux concepteurs de nouvelles applications (par exemple des architectes ICT), aux analystes, aux juristes d'entreprises, aux personnes qui prennent des décisions stratégiques en matière de développement de projets, aux responsables de la sous-traitance, aux responsables de la gestion du personnel, aux membres du personnel (ou à leurs représentants) qui utiliseront les données à caractère personnel en question dans l'exercice de leurs tâches, etc. ». CPVP, *Recommandation n° 01/2018*, *op. cit.*, pp. 27 et 28.

[274] Pour un exemple de présentation de cette répartition, la CPVP renvoie à Commission Nationale de l'Informatique et des Libertés (CNIL), « Privacy Impact Assessment (PIA) – Methodology (how to carry out a PIA) », 2015, p. 9. Voy. CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 28.

[275] La CPVP illustre une telle division des rôles aux pages 28 et 29 de sa *Recommandation n° 01/2018*, *op. cit.*

directement sur le sous-traitant. Dans la version finale du RGPD, il est toutefois précisé que le contrat entre le responsable du traitement et le sous-traitant doit établir que le sous-traitant « aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant »[276]. Le considérant n° 95 du RGPD confirme que le sous-traitant doit aider le responsable du traitement, « si nécessaire et sur demande », à assurer le respect des obligations découlant de la réalisation d'une AIPD[277].

§ 3. Le délégué à la protection des données

40. Lorsqu'un délégué à la protection des données (ci-après « DPD ») a été désigné, celui-ci a pour mission de conseiller le responsable du traitement dans l'exécution d'une AIPD[278]. Toutefois, le but n'est pas que le délégué à la protection des données rédige seul l'intégralité d'une AIPD[279]. Son rôle purement consultatif – et non décisionnel[280] – devrait porter sur les aspects suivants :

- faut-il effectuer ou non une AIPD ;
- quelle méthodologie faut-il suivre lors de la réalisation d'une AIPD ;
- l'AIPD doit-elle être effectuée en interne ou être externalisée ;
- quelles garanties (dont les mesures techniques et organisationnelles) doivent être appliquées afin d'atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées ;
- la question de savoir si l'AIPD a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes au RGPD[281].

---

[276] Art. 28, § 3, f), du RGPD.

[277] Selon la CPVP, « Compte tenu des dispositions précitées, l'ampleur de l'obligation d'assistance du sous-traitant doit être déterminée à la lumière (1) de la nature du traitement ; (2) des informations mises à disposition du sous-traitant ; (3) de l'opportunité de l'aide du sous-traitant afin de parvenir à une analyse et à une gestion des risques correctes et de qualité ». CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 29.

[278] Art. 35, § 2, du RGPD.

[279] C'est ce qui ressort notamment de l'article 39, § 1, c), qui dispose que le délégué à la protection des données « dispense des conseils, sur demande, en ce qui concerne l'AIPD et vérifie son exécution ».

[280] Toute autre interprétation pourrait en outre donner lieu à un conflit d'intérêts. « Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel ». Groupe 29, WP 243, *op. cit.*, p. 20.

[281] *Ibid.*

Si le responsable du traitement n'est pas d'accord avec l'avis rendu par le délégué à la protection des données, il motiver spécifiquement et par écrit dans la documentation de l'AIPD les raisons pour lesquelles il n'a pas été tenu compte de cet avis[282].

§ 4. Les personnes concernées ou leurs représentants

41. L'article 35, § 9, du RGPD dispose que « *le cas échéant*, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement »[283].

Par conséquent, l'APD belge « estime que l'idée derrière la formulation choisie est univoque, plus précisément que la décision de procéder ou non à la consultation des personnes concernées (ou de leurs représentants) revient en premier lieu au responsable du traitement. Il n'est toutefois pas entièrement facultatif pour le responsable du traitement de consulter ou non les personnes concernées ou leurs représentants. Là où il existe suffisamment de motifs importants de procéder à une telle consultation, compte tenu de la nature, du contexte, de la portée et de la finalité du traitement, ainsi que de l'impact potentiel sur les personnes concernées, il est nécessaire qu'une telle consultation ait effectivement lieu. Une consultation des personnes concernées est en particulier recommandée lorsqu'elles disposent d'informations essentielles ou qu'elles peuvent formuler des remarques importantes qui sont pertinentes pour la réalisation de l'AIPD. Si le responsable du traitement juge qu'il n'est pas approprié de demander l'avis des personnes concernées, par exemple parce que cela compromettrait la confidentialité de plans d'affaires ou serait disproportionné ou irréalisable, il doit documenter sa motivation de ne pas s'enquérir de l'avis des personnes concernées »[284].

---

[282] *Ibid.* Le Groupe 29 conseille par ailleurs que le responsable du traitement fixe clairement, par exemple dans le contrat du délégué à la protection des données, mais aussi dans les informations fournies aux travailleurs, au management (et à d'autres personnes concernées, au besoin), les tâches précises du délégué à la protection des données et leur ampleur, notamment en ce qui concerne la réalisation d'une analyse d'impact relative à la protection des données.

[283] La CPVP fait remarquer que la lecture séparée des versions anglaise, française et néerlandaise de l'article 35, § 9, du RGPD pourrait donner lieu à des interprétations divergentes : « Là où la version néerlandaise indique que la consultation des personnes concernées ou de leurs représentants doit se faire "in voorkomend geval", le texte anglais indique qu'une telle consultation doit se faire "where appropriate". Le texte français indique quant à lui "le cas échéant" ». CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 31.

[284] *Ibid.* Voy. égal. Groupe 29, WP 248, *op. cit.*, pp. 18 et 19.

Selon la CPVP, la consultation de personnes concernées ou de leurs représentants peut présenter une plus-value importante, tant lors de l'identification et de l'évaluation des risques du traitement que lors de la finalisation d'une AIPD, afin de vérifier si tous les risques ont été suffisamment cernés. L'ampleur de la consultation (quelles personnes ainsi que leur nombre) sera déterminée de préférence en fonction du risque et de l'ampleur du traitement. Si un traitement envisagé n'entraîne des risques que pour un nombre limité de personnes concernées (par exemple les travailleurs d'une petite organisation), la consultation peut se limiter à un nombre restreint de ces travailleurs et/ou de leurs représentants. Si le traitement envisagé implique des risques pour un grand nombre de personnes concernées (par exemple tous les habitants), il convient alors d'organiser une consultation plus large[285].

Le responsable du traitement décide en principe librement de la manière dont les personnes concernées ou leurs représentants sont consultés. Leur avis peut être recueilli de différentes manières, selon le contexte (par exemple une étude générique relative aux finalités et aux moyens du traitement, une question adressée aux représentants du personnel ou des enquêtes habituelles qui sont envoyées aux futurs clients du responsable du traitement)[286].

Si la décision finale du responsable du traitement diffère de l'avis des personnes concernées, il y a lieu qu'il documente les raisons de sa décision de persévérer ou non[287].

SECTION 4. – Éléments essentiels d'une AIPD

§ 1. Aperçu

42. L'article 35, § 7, du RGPD prévoit qu'une AIPD doit au moins contenir les éléments suivants :

a) *une description systématique des opérations de traitement envisagées et des finalités du traitement*, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;

b) une *évaluation de la nécessité et de la proportionnalité* des opérations de traitement au regard des finalités ;

c) une *évaluation des risques* pour les droits et libertés des personnes concernées ; et

---

285 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 32.
286 *Ibid.* Voy. égal. Groupe 29, WP 248, *op. cit.*, p. 18.
287 Art. 35, § 2, du RGPD. Voy. égal. Groupe 29, WP 248, *op. cit.*, p. 17.

d) *les mesures envisagées pour faire face aux risques*, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

§ 2. Description des opérations de traitement envisagées

43. L'article 35, § 7, du RGPD exige en premier lieu que l'AIPD contienne une description systématique des opérations de traitement envisagées et des finalités du traitement. Il est important que l'on tienne compte à cet égard de la nature, de la portée, du contexte, des finalités du traitement ainsi que des sources des risques[288]. Par conséquent, le Groupe 29 considère que la description des traitements doit comporter au moins les éléments suivants :

- une description claire du traitement, y compris d'éventuels processus d'entreprise et exigences du système ;
- les données à caractère personnel, les destinataires et la durée pendant laquelle les données à caractère personnel seront enregistrées ;
- les actifs sur lesquels reposent les données à caractère personnel (par exemple matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier)[289].

Pour un aperçu d'autres éléments pertinents pour déterminer la nature, la portée et le contexte des traitements, nous renvoyons le lecteur à la section 4 de la présente contribution.

§ 3. Contrôle de la nécessité et de la proportionnalité

44. Une AIPD doit comporter une évaluation de la *nécessité et de la proportionnalité* des opérations de traitement au regard des finalités. Le responsable du traitement doit dès lors justifier explicitement, d'une part, pour quelle(s) raison(s) le traitement de données à caractère personnel est nécessaire et, d'autre part, pour quelle(s) raison(s) chacun des traitements visés est nécessaire pour atteindre la (les) finalité(s) poursuivie(s).

Lors de l'évaluation de la nécessité, si plusieurs traitements ou moyens de traitement sont utilisés pour atteindre la (les) finalité(s), le responsable du traitement doit en principe choisir les moyens de traitement qui sont

[288] Voy. égal. considérant n° 90 du RGPD.
[289] Groupe 29, WP 248, *op. cit.*, p. 28.

les moins intrusifs. Le responsable du traitement a alors intérêt à bien documenter la (les) raison(s) pour laquelle (lesquelles) les moyens de traitement choisis sont moins intrusifs que les alternatives[290].

Lors de l'évaluation de la proportionnalité, le responsable du traitement doit également examiner la *pertinence* du traitement envisagé. En somme il s'agit de répondre à la question « peut-on raisonnablement espérer que le traitement envisagé atteindra sa finalité (légitime) » ? Enfin, le responsable du traitement doit aussi veiller à maintenir un équilibre adéquat entre les intérêts pertinents[291].

Par conséquent, lors de l'évaluation de la nécessité et de la proportionnalité du traitement envisagé, il faut tenir compte au moins des éléments suivants :

- la (les) finalité(s) spécifiée(s), explicite(s) et légitime(s) du traitement envisagé ;
- le fondement juridique sur lequel se base le traitement de données[292] ;
- une justification du fait que les données à caractère personnel traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire[293] ;
- une justification du délai de conservation envisagé des données à caractère personnel, qui ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[294] ;
- une justification du fait que les intérêts de la personne concernée ne prévalent pas sur les intérêts légitimes du responsable du traitement ou d'éventuels tiers.

En outre, il est également recommandé que le responsable du traitement propose un relevé de toutes les mesures techniques et organisationnelles prises pour remplir les obligations de sécurité. En effet, au moment de l'exécution de l'AIPD, le responsable du traitement qui la réalise aura peut-être déjà

---

[290] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 17.

[291] L'évaluation de l'équilibre d'intérêts à ce stade de l'AIPD ne sera généralement que provisoire, étant donné qu'elle ne tient pas encore compte des mesures de protection visées. Groupe 29, WP 248, *op. cit.*, p. 28.

[292] Art. 6 du RGPD. En principe, une opération de traitement qui ne poursuit qu'une seule finalité ne peut être justifiée qu'à l'aide d'un seul des fondements juridiques repris à l'article 6 du RGPD. « Il est toutefois possible qu'un même traitement poursuive plusieurs finalités. Dans ce cas, il est possible que plus d'un fondement juridique entre en considération pour justifier le traitement de données envisagé ». Groupe 29, Guidelines for consent under 2016/679, WP 259, 28 novembre 2017, p. 22.

[293] Art. 5, § 1, c), du RGPD.

[294] Art. 5, § 1, e), du RGPD.

pris plusieurs mesures pour respecter ses obligations. Ces mesures existantes peuvent avoir une influence sur l'évaluation des risques pour les droits et libertés des personnes physiques. Il est dès lors important que celles-ci soient documentées, afin qu'elles puissent aussi être prises en compte lors de l'évaluation et de la détermination des risques résiduels finaux[295]. Enfin, la CPVP s'attend à ce que l'AIPD fournisse également un aperçu des mesures qui contribuent aux droits des personnes concernées[296], de la manière dont les relations avec les sous-traitants sont régies[297] ainsi que, le cas échéant, des garanties concernant le (les) transfert(s) international (internationaux) qui seront prévues[298].

§ 4. L'évaluation des risques dans le cadre d'une AIPD

45. En ce qui concerne l'évaluation des risques dans le cadre d'une AIPD, les considérants n^os^ 84 et 90 du RGPD précisent que celle-ci vise en premier lieu les risques « élevés ». Si, par exemple, lors d'un traitement déterminé, il y a un risque élevé d'atteinte à la réputation mais qu'il n'y a qu'un très faible risque de discrimination, ce dernier risque ne doit pas *nécessairement* être repris en tant que tel dans l'évaluation des risques d'une AIPD. Néanmoins, la CPVP recommande, dans le cadre d'une AIPD, de cartographier expressément tous les risques qui ne sont pas négligeables et d'identifier des mesures de protection efficaces, étant donné que même des risques moyens peuvent constituer un facteur important lors de l'évaluation de *la nécessité et de la proportionnalité* du traitement de données envisagé. Quoi qu'il en soit, une AIPD doit comporter un relevé de toutes les mesures prises afin d'apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. Dans cette optique également, il est important que tous les risques pertinents soient pris en compte.

Dans l'annexe 2 de ses lignes directrices, le Groupe 29 énumère les critères qui peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD ou une méthodologie d'AIPD est considérée comme suffisamment complète aux fins du respect des exigences du RGPD[299]. Le Groupe rappelle également qu'un certain nombre de cadres

---

[295] Groupe 29, WP 248, *op. cit.*, p. 7.

[296] Dont l'information communiquée à la personne concernée (art. 12, 13 et 14 du RGPD) ; le droit d'accès et le droit à la portabilité des données (art. 15 en 20 du RGPD) ; le droit de rectification et le droit à l'effacement de données (art. 16, 17 et 19 du RGPD) ; le droit d'opposition et le droit à la limitation du traitement (art. 18, 19 et 21 du RGPD.

[297] Art. 28 du RGPD.

[298] Groupe 29, WP 248, *op. cit.*, p. 28.

[299] *Ibid.*, p. 26.

développés par les autorités de contrôle de l'UE ainsi que de cadres sectoriels européens ont été publiés[300].

§ 5. Consultation préalable de l'autorité de contrôle

46. L'article 36, § 1, du RGPD dispose que « le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ». Il ressort de la formulation de cet article qu'une consultation préalable n'est obligatoire que lorsque le risque résiduel est élevé. Une consultation préalable n'est donc requise que lorsque l'AIPD démontre que le traitement va de pair avec un risque élevé que le responsable du traitement ne peut l'atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre. Si le risque peut être limité efficacement à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable ne doit avoir lieu[301].

Selon le Groupe 29, un risque résiduel élevé inacceptable existe par exemple lorsqu'il est probable que les personnes concernées soient confrontées à des conséquences considérables ou irréversibles (par exemple un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière). Il semble ainsi évident que le risque se concrétisera dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée[302].

Si l'autorité de contrôle estime que le traitement envisagé n'est pas conforme au RGPD ou que les risques ne sont pas suffisamment identifiés ou atténués, elle fournit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58 du RGPD, y compris le pouvoir d'imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement[303]. Ce délai de 8 semaines peut être prolongé de 6 semaines[304]. Ces

[300] *Ibid.*, p. 24.
[301] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 26.
[302] Groupe 29, WP 248, *op. cit.*, p. 22
[303] Art. 58, § 2, e), du RGPD.
[304] Dans le cas d'une telle prolongation, l'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard notamment, dans un délai d'un mois à compter de la réception de la demande de consultation.

délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation[305].

Lorsqu'une consultation préalable est obligatoire, le responsable du traitement doit fournir les informations suivantes[306] :

- le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;
- les finalités et les moyens du traitement envisagé ;
- les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du RGPD ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- l'analyse d'impact relative à la protection des données prévue à l'article 35 du RGPD ;
- et, toute autre information demandée par l'autorité de contrôle.

Enfin, rappelons que l'autorité de contrôle doit en général être consultée lors de la préparation d'une mesure législative ou réglementaire qui concerne la protection des données à caractère personnel[307].

[305] Art. 36, § 2, du RGPD.

[306] Art. 36, § 3, du RGPD.

[307] Art. 36, § 4, et 57, § 1, c), du RGPD. De plus, conformément à l'article 36, § 5, du RGPD, « le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique ».

CHAPITRE 8. Les mesures techniques et organisationnelles appropriées

SECTION 1. – La politique de la sécurité de l'information

47. Qu'une AIPD soit effectuée ou non, dans l'objectif d'être en mesure de démontrer que le traitement est conforme à l'obligation de sécurité, l'article 24, § 2, du RGPD astreint le responsable du traitement à mettre en œuvre, lorsque cela est proportionné, *des politiques appropriées* en matière de protection des données. Dans le même esprit, le règlement considère que

celui-ci « devrait adopter *des règles internes* et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut »[308]. De plus, ainsi que nous l'avons déjà mentionné, le responsable du traitement ne peut faire appel qu'à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

C'est à la lumière de ces prescrits que doit être lue la recommandation de la CPVP selon laquelle « tout organisme traitant des données à caractère personnel doit rédiger un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser ces données »[309]. Celle-ci comprendra utilement :

- l'exposé de la démarche d'évaluation des risques relatifs aux données à caractère personnel ;
- les priorités retenues et les mécanismes mis ou à mettre en place consécutivement à cette analyse des risques ;
- le planning de mise en œuvre ;
- la description des différentes responsabilités et des règles organisationnelles mises en place ;
- la description du processus de gestion des incidents de sécurité ;
- la description du processus de sensibilisation de l'organisme à cette politique ;
- les dispositions retenues afin de maintenir à jour le système de sécurisation une fois installé.

Enfin, cette politique de sécurité de l'information devrait être « approuvée par le plus haut niveau de la hiérarchie ainsi que par les divers responsables et suffisamment diffusée au sein de l'organisme afin d'être connue de tous »[310].

SECTION 2. – Méthodologie de l'évaluation des risques

48. Ainsi que nous l'avons déjà mentionné à plusieurs reprises, qu'une AIPD soit effectuée ou non, l'article 32 du RGPD impose aux débiteurs de l'obligation de sécurité d'évaluer les risques inhérents au traitement et mettre en œuvre des mesures pour les atténuer. Afin de se livrer

[308] Considérant n° 78 du RGPD.

[309] CPVP, *Mesures de référence applicables à tout traitement de données à caractère personnel*, *op. cit.*, p. 2.

[310] *Ibid.*

à l'exercice d'évaluation du risque, les débiteurs de l'obligation de sécurité peuvent choisir librement la méthode qu'ils souhaitent appliquer, à condition qu'elle soit objective et que le choix de l'une ou l'autre méthode puisse être justifié, compte tenu de la nature, du champ d'application, du contexte et des finalités du traitement[311]. Néanmoins, dans le but d'éviter qu'une situation d'insécurité juridique ne survienne, la CPVP a formulé plusieurs caractéristiques minimales d'une bonne gestion des risques[312].

Outre le fait que la gestion des risques doit, entres autres, être étayée méthodologiquement[313], être adaptée sur mesure au contexte et au profil du débiteur de l'obligation de sécurité, être lisible et accessible à un public aussi large que possible, elle doit également être structurée de manière à contenir notamment :

- la définition du contexte pertinent (incluant une description de l'objet de l'analyse de risque, une définition des critères servant à évaluer les risques pour les droits et libertés des personnes physiques et la définition de valeurs de risques (in)acceptables) ;
- l'identification, analyse et évaluation des risques (y compris l'identification des vulnérabilités, des menaces et l'attribution d'une valeur de risque) ; et
- l'identification de mesures d'atténuation des risques appropriées (c'est-à-dire les mesures techniques, organisationnelles et juridiques qui sont nécessaires pour ramener le risque à un niveau acceptable).

De plus, la méthode de gestion de risques doit être suffisamment nuancée et « comporter suffisamment d'échelles afin de permettre une évaluation nuancée des risques identifiés. Ne prévoir que trois échelles (bas, moyen, élevé) pour apprécier les risques n'est pas toujours suffisant pour donner lieu à une appréciation correcte. Une description claire des critères utilisés pour évaluer le risque est quoi qu'il en soit indispensable »[314].

Selon la CPVP il y a également lieu d'impliquer ceux qui sont les mieux placés pour contribuer au processus d'identification, d'analyse,

311 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 23.

312 *Ibid.*, « Annexe 1 : Caractéristiques minimales d'une bonne gestion des risques », pp. 39 à 41.

313 En outre, la CPVP recommande vivement « de se baser sur des méthodes déjà existantes en matière de gestion des risques. L'utilisation de normes internationales, telles que celles développées par l'Organisation internationale de normalisation (ISO). En particulier la norme ISO 31000 (Risk management). ISO 27005 (Information security risk management) et ISO/IEC 29134 (Guidelines for privacy impact assessment). L'adhésion à des codes de conduite élaborés ou agréés au niveau européen, est particulièrement importante dans ce cadre également ». CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 23.

314 CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 41.

d'évaluation et de gestion des risques : « ce groupe comprend non seulement le délégué à la protection des données et/ou le conseiller en sécurité mais également les concepteurs de nouvelles applications, ceux qui prennent des décisions stratégiques en matière de développement de projets et les membres du personnel (ou leurs représentants) qui utiliseront les données à caractère personnel en question dans le cadre de l'exercice de leurs missions »[315].

Enfin, des mesures de gestion et de contrôle devraient être prévues : « un rapport daté et écrit des appréciations du risque effectuées doit être rédigé. Un organe interne mandaté qui prend des décisions (par exemple le comité de direction, le comité stratégique ou le comité de sécurité, mandaté par le conseil de direction) doit être informé périodiquement du résultat (ou du statut) du processus d'appréciation du risque. Cet organe mandaté doit approuver formellement l'évaluation des risques ainsi que les mesures visant à atténuer les risques. Le processus d'appréciation du risque ne peut toutefois pas être réduit à un simple processus bureaucratique. Le responsable du traitement doit prendre des mesures adéquates afin de veiller à ce que la bonne gestion des risques fasse partie de la "culture d'entreprise" du responsable du traitement.

Une appréciation du risque qui a été effectuée doit être contrôlée périodiquement et au moins en cas de circonstances changeantes pouvant avoir une influence essentielle sur une appréciation qui a été réalisée dans le passé. La fréquence de la vérification périodique doit être déterminée en fonction du risque présenté par l'opération de traitement. En outre, la Commission recommande également que le résultat du contrôle soit officiellement soumis à l'approbation de la plus haute autorité au sein de l'organisation du responsable du traitement »[316].

SECTION 3. – L'état des connaissances et les coûts de mise en œuvre

49. Outre la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, l'article 32, § 1, du RGPD énumère deux facteurs supplémentaires qui doivent être pris en compte pour assurer la mise en œuvre de mesures de sécurité appropriées, à savoir

315 *Ibid.*
316 *Ibid.*

« l'état des connaissances et les coûts de mise en œuvre »[317]. Aucune hiérarchisation de ces critères n'est établie par le règlement, de sorte qu'aucun de ceux-ci n'a expressément de primauté sur l'autre.

Néanmoins, en ce qui concerne la référence légale aux coûts, Y. Poullet insiste sur le fait que celle-ci « ne peut se concevoir en fonction des ressources financières du responsable du traitement. Les frais doivent être suffisants et raisonnables compte tenu des précédents critères. Il serait inacceptable qu'un responsable des traitements limite la sécurité de son système d'information nonobstant les risques encourus pour les personnes concernées au seul motif que les techniques disponibles sont trop onéreuses au regard de ses ressources financières »[318]. La CPVP va dans le même sens en estimant que « le coût de la mise en place des mesures de sécurité doit évidemment être évalué en comparaison des conséquences que pourrait avoir un incident de sécurité dû à une absence de protection »[319]. Toutefois, « le coût des mesures envisagées ne peut pas en soi constituer une raison de réaliser un traitement sans garanties suffisantes. Si le responsable du traitement n'est pas en mesure de prévoir des garanties suffisantes et de ramener le risque à un niveau acceptable, au vu de la technologie disponible et des frais d'exécution, il doit le cas échéant soit renoncer au traitement, soit réaliser une consultation préalable de l'autorité de contrôle »[320].

Quant à la prise en compte de l'état des connaissances, celle-ci doit se lire, selon Y. Poullet comme une obligation de « s'informer des diverses techniques de sécurité présentes sur le marché et à les évaluer à l'aune des risques décelés »[321]. Dans la même logique, le Conseil de l'Europe recommande que « les mesures de sécurité devraient prendre en considération les méthodes et techniques *de pointe* en matière de sécurité des données dans le cadre du traitement de données »[322].

---

[317] Art. 32, § 1, du RGPD.

[318] Y. Poullet, « La sécurité informatique, entre technique et droit », *op. cit.*, p. 43.

[319] CPVP, « note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 9.

[320] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 25.

[321] Y. Poullet, « La sécurité informatique, entre technique et droit », *op. cit.*, p. 43. L'auteur insiste sur le fait que ces techniques doivent être présentes sur le marché comme produits déjà commercialisés et non encore à l'état de prototypes et donc difficilement disponibles.

[322] Conseil de l'Europe, Rapport explicatif de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 2018, pt 63

SECTION 4. – Mesures de sécurité, codes de conduite et certifications

§ 1. Objet

50. En ce qui concerne la nature des mesures de sécurité devant être mises en œuvre par les débiteurs de l'obligation de sécurité, le règlement en distingue deux types : d'une part, les mesures techniques, d'autre part les mesures organisationnelles.

En 1990, la Commission européenne précisait déjà le contour de ces notions : « *technical measures of data security include : safety measures for access to data processing and storage locations, identification codes for persons entitled to enter such locations, informational safeguards such as the use of passwords for access to electronically processed files, the enciphering of data and monitoring of hacking and other unusual activities. Through organizational measures, the controller of the file adopts certain procedural stops within the hierarchy of his public authority or business enterprise, e.g. by establishing authority levels with regard to access to the data* »[323].

La CPVP opère, quant à elle, la distinction suivante entre mesures techniques, organisationnelles ou juridiques[324] :

- Mesures organisationnelles : accroissement de la conscientisation, formation, mesures politiques, séparation des fonctions (ce qu'on appelle "Muraille de Chine"), rapport, contrôles périodiques, possibilités supplémentaires de choix, de participation ou d'opposition pour les personnes concernées, etc. ;
- Mesures techniques : limitations techniques à la collecte et/ou à la communication de données à caractère personnel (par exemple utilisation de techniques cryptographiques particulières pour faire de la minimalisation de données), l'anonymisation, la pseudonymisation et/ou le cryptage de données à caractère personnel après leur collecte, les limitations techniques à la réutilisation de données à caractère personnel (finalité), l'authentification multifacteurs, la journalisation et le monitoring, la scission de données, les sauvegardes supplémentaires, etc. ;
- Mesures juridiques : garanties contractuelles, règles d'entreprise contraignantes, etc.

---

[323] Commission communication on the protection of individuals on relation to the processing of personal data in the Community and Information security, COM (90) 314 final, 13 September 1990, p. 37.

[324] CPVP, *Recommandation n° 01/2018*, *op. cit.*, p. 24.

§ 2. Codes de conduite et certifications

51. Selon l'article 32, § 3, du RGPD, « l'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues [par le paragraphe premier dudit article] »[325]. De plus le règlement considère que « des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de codes de conduite approuvés, de certifications approuvées et de lignes directrices données par le comité ou d'indications données par un délégué à la protection des données »[326]. Dans le cadre de la présente contribution, nous n'analysons pas ces importantes thématiques. À titre purement indicatif nous renvoyons le lecteur aux recommandations relatives à la certification en matière de protection des données publiées par l'ENISA en novembre 2017[327].

SECTION 5. – Aperçu de quelques mesures de sécurité techniques

52. Dans les sections qui suivent, nous ne prétendons à aucune exhaustivité ni dans l'énumération ni dans la description des mesures des sécurité techniques et organisationnelles opportunes, celles-ci dépendant fortement de l'identification des risques inhérents à atténuer. Nous nous limitons donc à mettre l'accent sur certaines de celles-ci, soit parce qu'elles sont expressément mentionnées dans le RGPD, soit parce qu'elles sont recommandées par des autorités de contrôle.

---

[325] Dans le même esprit, l'article 24, § 3, du RGPD dispose que « l'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement ».

[326] Considérant n° 77 du RGPD.

[327] ENISA, *Recommendations on European Data Protection Certification*, version 1.0, novembre 2017, disponible à l'adresse
https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport.

§ 1. L'anonymisation

53. À titre liminaire, rappelons que le RGPD ne s'applique pas au traitement de données anonymes, à savoir « les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable »[328]. Toutefois, le processus d'anonymisation en lui-même constitue un traitement de données à caractère personnel ; et à ce titre, il est soumis aux exigences du règlement jusqu'au moment où les données sont effectivement rendues anonymes[329]. Les principales techniques d'anonymisation, à savoir la randomisation et la généralisation ont été décrites par le Groupe 29[330].

À l'issue du processus d'anonymisation, afin de vérifier si les données permettent l'identification d'une personne physique et si ces informations peuvent être considérées comme anonymes ou pas, l'exposé des motifs de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui transposait la Directive (la « LVP ») dispose qu'« elles ne perdent leur caractère de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen raisonnablement susceptible d'être mis en œuvre ne permet de revenir en arrière pour briser l'anonymat »[331]. L'exposé des motifs de la Recommandation n° R (97)18[332] abonde dans le même sens concernant la question des moyens raisonnables permettant une réidentifcation : « le risque de réidentification ne doit pas être strictement nul, on peut considérer qu'il est nul en pratique lorsque la réidentification demanderait des opérations excessivement compliquées, longues et coûteuses. Aucun coffre-fort n'est rigoureusement inviolable ; on doit exiger des précautions qui rendent la violation non pas strictement impossible, mais très improbable. Et cette exigence peut varier selon la nature des données, selon qu'elles sont plus ou moins sensibles ». En pratique, pour savoir si des données peuvent être considérées comme anonymes, il faut donc procéder à un examen au cas par cas pour tenir compte de toutes les circonstances. Cela s'avère particulièrement important dans le cas des

---

[328] Considérant n° 26 du RGPD.

[329] Groupe 29, Avis 05/2014 sur les techniques d'anonymisation, WP 216, adopté le 10 avril 2014, p. 3.

[330] *Ibid.*

[331] Exposé des motifs de la loi du 11 décembre 1998, *Doc. parl.*, Ch., sess. ord. 1997-1998, n° 1566/1, p. 12.

[332] Recommandation (97)18 du Conseil de l'Europe sur la protection des données à caractère personnel, collectées et traitées à des fins statistiques, adoptée par le Comité des Ministres le 30 septembre 1997.

informations statistiques où, en dépit du fait que lesdites informations peuvent se présenter sous forme agrégée, l'échantillon initial n'est pas suffisamment important si d'autres éléments d'information peuvent permettre d'identifier les personnes physiques[333]. Par conséquent, à défaut d'être absolument certains d'avoir à faire à des données réellement anonymes, nous recommandons aux débiteurs de l'obligation de sécurité de les considérer comme restant « à caractère personnel ».

§ 2. La pseudonymisation

54. La « pseudonymisation » est définie par le RGPD comme étant « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[334]. Concrètement, la pseudonymisation consiste à donc remplacer un attribut (généralement un attribut unique) par un autre dans un enregistrement afin de réduire le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée qui reste, par conséquent, toujours susceptible d'être identifiée indirectement[335]. Le résultat de la pseudonymisation peut être indépendant de la valeur initiale (comme dans le cas d'un numéro aléatoire généré par le responsable du traitement ou d'un nom choisi par la personne concernée) ou il peut être dérivé des valeurs originales d'un attribut ou d'un ensemble d'attributs, par exemple au moyen d'une fonction de hachage ou d'un système de chiffrement[336]. Certaines techniques de pseudonymisation ont été décrites et analysées par le Groupe 29 dans un avis de 2014[337].

Sous le régime de la LVP, les données pseudonymisées étaient désignées sous l'appellation de « données codées ». Celles-ci étaient définies comme étant « des données à caractère personnel qui ne peuvent être mises en relation avec une personne identifiée ou identifiable qu'au moyen d'un code »[338]. L'exposé des motifs de la loi précisait que doivent également

333 Groupe 29, WP 136, *op. cit.*, p. 23.
334 Art. 4, 5), du RGPD.
335 Groupe 29, WP 216, *op. cit.*, p. 22.
336 *Ibid.*
337 *Ibid*, pp. 23 à 25.
338 Art. 1er, § 1er, 3°, A.R. 13 février 2001, *op. cit.*

être considérées comme données à caractère personnel « les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne »[339]. De la même manière, sous l'empire du RGPD, les données pseudonymisées sont par définition des données relatives à un individu identifiable, du fait que le lien entre le pseudonyme et les données d'identification (par exemple, nom, prénom, adresse postale, adresse IP...) est disponible pour l'organisation collectant l'information ou une tierce partie[340]. Par ailleurs, le RGPD considère que « des mesures de pseudonymisation devraient être possibles chez un même responsable du traitement, tout en permettant une analyse générale, lorsque celui-ci a pris les mesures techniques et organisationnelles nécessaires afin de garantir, pour le traitement concerné, que le présent règlement est mis en œuvre, et que les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise soient conservées séparément »[341]. Dans ce cas, le responsable du traitement qui traite les données à caractère personnel devrait indiquer les personnes autorisées à cet effet chez un même responsable du traitement.

L'intérêt de procéder à la pseudonymisation n'est donc pas de déroger à la l'application du RGPD mais de réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de sécurité des données[342]. Notons toutefois que l'introduction explicite de la pseudonymisation dans le RGPD ne vise pas à exclure d'autres mesures de sécurité des données, comme par exemple le chiffrement[343].

§ 3. Le chiffrement

55. Contrairement à la Directive qui ne mentionnait pas le chiffrement, le RGPD fait y explicitement référence sans toutefois le définir. Néanmoins, en Belgique, son usage est régulé par l'article 48 du la loi du

339 Exposé des motifs de la loi du 11 décembre 1998, *op. cit.*

340 Le considérant n° 26 du RGPD indique expressément que « les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».

341 Considérant n° 29 du RGPD.

342 L'usage de la pseudonymisation peut également être utile dans le cadre de l'application de l'article 11 du RGPD.

343 Considérant n° 28 du RGPD.

13 juin 2005 qui dispose que « l'emploi de la cryptographie est libre »[344]. Dans ce contexte, la notion y est définie comme « l'ensemble des services mettant en œuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée »[345].

56. Premièrement, selon le Groupe 29, « le cryptage peut contribuer de manière significative à la confidentialité des données à caractère personnel s'il est utilisé correctement, bien qu'il ne rende pas les données à caractère personnel irréversiblement anonymes ». Le Groupe 29 accorde une importance essentielle au chiffrement puisque celui-ci estime que « le cryptage des données à caractère personnel devrait être systématique pour les données "en transit" et être utilisé lorsque c'est possible pour les données "au repos" »[346]. Le Groupe recommande également de stocker les mots de passe « de manière sécurisée (par exemple, par salage ou à l'aide d'une fonction de hachage à clé cryptographique) »[347]. Utilisé de cette manière, en sus de mettre en place une garantie appropriée de sécurité, l'intérêt pour le responsable du traitement de procéder au chiffrement de données, en les rendant incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, est d'être *dans certaines circonstances*[348] dispensé de son obligation de communiquer une violation de telles données aux personnes concernées[349] et par conséquent d'être davantage à l'abri d'une perte de confiance de celles-ci.

57. Un second avantage de l'utilisation du chiffrement, tant pour le responsable du traitement que pour les personnes concernées, est « de recourir à des mécanismes d'authentification cryptographiques tels que les codes

[344] Art. 48 de la loi du 13 juin 2005 relative aux communications électroniques. Néanmoins, le même article précise que « la fourniture au public de services de cryptographie que le Roi détermine, après avis de l'Institut [IBPT], est soumise à une déclaration préalable auprès de l'Institut. Le Roi arrête, après avis de l'Institut, le contenu et la forme de cette déclaration ». À notre connaissance, un arrêté royal n'a pas encore été adopté à ce sujet.

[345] Art. 2, 40°, de la loi du 13 juin 2005 relative aux communications électroniques. À cet égard, l'OCDE souligne que « l'utilisation de la cryptographie pour garantir l'intégrité des données, y compris les mécanismes d'authentification et de non-répudiation, peut être distinguée de son utilisation pour garantir la confidentialité des données, et que chacune de ces utilisations pose des problèmes différents ». OCDE, *Recommandation du conseil relative aux lignes directrices régissant la politique de cryptographie*, 22 mars 1997, p. 4.

[346] Groupe 29, WP 196, *op. cit.*, p. 18.

[347] Groupe 29, WP 213, *op. cit.*, p. 10.

[348] Voy. la section 5 du chapitre 9 de la présente contribution.

[349] Art. 34, § 3, a), du RGPD.

ou signatures d'authentification des messages afin de détecter les modifications apportées aux données à caractère personnel »[350]. De telles pratiques peuvent s'avérer extrêmement utiles afin de compléter judicieusement des politiques d'accès logiques aux données[351]. À titre indicatif, mentionnons que des études relatives aux méthodes de chiffrement dans le contexte de la protection des données à caractère personnel ont été publiées par l'ENISA[352].

§ 4. La sécurité des réseaux

58. L'évolution de la technologie et de l'interconnexion entre les systèmes d'informations, la dématérialisation des dits systèmes ainsi que de leurs supports ne font qu'accroître les risques de violations de données. Selon la CPVP, « la disponibilité inadéquate de données à caractère personnel sur Internet constitue un problème majeur, et ce d'autant plus que ces données peuvent avoir une valeur marchande et que leur diffusion en devient incontrôlable à l'heure actuelle si des mesures de sécurité appropriées ne sont pas prises »[353]. Par conséquent, l'APD belge considère que lorsque « le réseau interne de l'organisme est connecté à un réseau externe public, l'organisme doit prendre les mesures nécessaires afin de protéger le ou les réseaux impliqué(s) dans le traitement des données à caractère personnel contre tout accès non autorisé »[354], qu'il s'agisse de menaces (actions extérieures ou intérieures malveillantes) ou de vulnérabilités (risques propres aux systèmes et applications).

À cet égard, l'autorité recommande une architecture informatique locale « basée sur le principe des couches de sécurité, en implémentant une segmentation logique et/ou physique des zones. L'accès direct aux systèmes applicatifs depuis Internet sera contrecarré par l'utilisation simultanée de divers moyens disponibles selon les cas, par exemple des serveurs relais tels "Proxy/Reverse Proxy", par la translation des adresses IP, par un pare-feu (firewall) ou un routeur convenablement paramétrés »[355]. En fonction

---

[350] Groupe 29, WP 196, *op. cit.*, p. 18.

[351] Voy. le § 3, de la section 6 du chapitre 8 de la présente contribution.

[352] L'ENISA a publié, entre autres, le document « Recommended cryptographic measures – Securing personal data » le 20 septembre 2013 ; le document « Algorithms, Key Sizes and Parameters Report – 2013 » le 29 octobre 2013 ; le document « Study on cryptographic protocols » le 21 novembre 2014 ; et enfin, le document « Updated Report on Algorithms, Key Sizes and Parameters » le 21 novembre 2014.

[353] CPVP, *Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*, *op. cit.*, p. 2.

[354] CPVP, *Mesures de référence applicables à tout traitement de données à caractère personnel*, *op. cit.*, p. 4.

[355] CPVP, *Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*, *op. cit.* p. 4.

des ressources disponibles, la mise en place et le suivi d'un système de détection (et de prévention) d'intrusion (IDS/IPS) sont un plus permettant de repérer des activités anormales ou suspectes[356].

SECTION 6. – Aperçu de quelques mesures de sécurité organisationnelles

§ 1. L'organisation et aspects humains de la sécurité de l'information

59. Il va de soi qu'une première mesure organisationnelle importante est la désignation d'un délégué à la protection des données dans les circonstances prévues par l'article 37 du RGPD. Dans de tels cas, celui-ci doit exercer les fonctions précisées dans l'article 38 du règlement et avoir pour missions celles énumérées à l'article 39 dont fait partie « le contrôle des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant »[357].

Qu'un délégué à la protection des données doive être désigné ou non, il est fortement recommandable que chaque débiteur de l'obligation de sécurité définisse clairement les responsabilités et processus de gestion en matière de sécurité des données à caractère personnel et les intègre adéquatement dans son organisation générale et son fonctionnement[358]. En effet, l'article 32, § 4, du RGPD impose explicitement tant au responsable du traitement qu'au sous-traitant de prendre des mesures afin de garantir que toute personne physique agissant sous leur autorité qui a accès à des données à caractère personnel, « *ne les traite pas, excepté sur instruction du responsable du traitement*, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre ». Dans le même esprit, l'article 28, § 3, b), du règlement impose au sous-traitant de veiller « à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ».

---

356 *Ibid.*

357 Art. 39, § 1, b), du RGPD.

358 CPVP, *Mesures de référence applicables à tout traitement de données à caractère personnel*, *op. cit.*, p. 3.

Par conséquent, la mise en place « de procédures de classification de l'information permettant d'inventorier et de localiser toutes les données à caractère personnel traitées, et ce, quel qu'en soit le support » est fortement recommandée[359].

La CPVP estime également que « la réussite de la sécurisation d'un système d'information dépendant fortement de l'information correcte des différents acteurs, l'organisme doit prendre les mesures nécessaires afin que toute personne (interne ou externe) intervenant dans le traitement des données personnelles soit constamment suffisamment informée de ses devoirs et responsabilités lors de ces traitements et suffisamment et correctement formée à l'exercice de sa fonction et de ses responsabilités de sécurité de l'information. D'éventuels suivis disciplinaires doivent être prévus en cas de non-respect des règles édictées et un engagement de confidentialité requis lorsque les risques le justifient »[360]. Enfin, il va de soi que lorsque l'organisme sous-traite tout ou partie de ses traitements, il veillera à répercuter, dans le contrat de sous-traitance, les obligations de sécurité qu'il estime opportunes[361].

§ 2. La sécurité physique et de l'environnement

60. Afin de garantir la protection physique des données à caractère personnel, il est fortement recommandable de s'assurer que les supports des données à caractère personnel et les systèmes informatiques soient placés, conformément à leur classification, dans des locaux identifiés et protégés et dont l'accès est limité aux seules personnes autorisées et aux seules heures justifiées par leur fonction[362].

L'APD belge estime également que, dans les cas où une continuité des services s'avère nécessaire, « des dispositifs de prévention, de détection et de traitement de dangers physiques tels que les incendies ou les inondations doivent être installés et régulièrement contrôlés. L'organisme doit aussi prendre les mesures de sauvegarde (back up) nécessaires afin de pouvoir contrer la perte ou l'altération accidentelle de données à caractère personnel »[363]. Ainsi que nous l'avons déjà mentionné, des références aux mesures garantissant, selon les besoins, la disponibilité et la résilience des données sont explicitement mentionnées dans l'article 32, § 1, du RGPD.

---

359 *Ibid.*

360 *Ibid.*

361 Voy. à ce sujet les sections 1 et 2 du chapitre 3 de la présente contribution.

362 CPVP, *Mesures de référence applicables à tout traitement de données à caractère personnel*, *op. cit.*, p. 3.

363 *Ibid*, p. 4.

§ 3. La sécurisation logique des accès

61. Une importante recommandation adressée aux débiteurs de l'obligation de sécurité et de « s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation »[364]. Selon le Groupe 29, « il convient d'attribuer à chaque personne son propre compte et l'accès aux données à caractère personnel devrait être exclusivement autorisé en appliquant les principes du besoin d'en connaître et de moindre privilège [...] ces personnes devraient uniquement avoir accès à la fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues, pour une durée qui se limite à ce qui est strictement nécessaire. L'utilisation des comptes disposant d'un "accès global" à la base de données devrait être limitée et des méthodes de traçage et de restriction de l'utilisation de ce type de comptes devraient être appliquées »[365]. À cet effet, il s'agit de maintenir à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction). Ces différentes autorisations « doivent être traduites en dispositifs techniques et contrôles d'accès aux différents éléments informatiques (programmes, procédures, éléments de stockage, équipements de communication, etc.) intervenant dans le traitement des données à caractère personnel »[366].

De plus, selon la CPVP, « si le niveau de sécurité l'impose, l'identification des intervenants sera complétée par une procédure d'authentification »[367]. La CNIL va dans le même sens en affirmant que « pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques »[368]. Les mécanismes permettant de réaliser l'authentification des personnes sont catégorisés selon qu'ils font intervenir :

- ce que l'on sait, par exemple un mot de passe ;
- ce que l'on a, par exemple une carte à puce ;
- une caractéristique qui nous est propre, par exemple une modalité biométrique[369].

---

364 *Ibid.*

365 Groupe 29, WP 213, *op. cit.*, p. 10.

366 *Ibid.*

367 *Ibid.*

368 CNIL, « La sécurité des données personnelles », *op. cit.*, p. 7.

369 Évidemment, une modalité biométrique étant considérée comme une donnée sensible au sens de l'article 9 du règlement, il s'agit d'appliquer le RGPD en fonction.

Par ailleurs, la CNIL qualifie l'authentification d'un utilisateur comme étant forte lorsqu'elle a recours à une combinaison d'au moins deux de ces catégories[370]. En outre, dès lors que des moyens d'authentification sont compromis, il s'agit « d'obliger les personnes concernées à créer un nouveau mot de passe, en mode sécurisé, afin de garantir que tous les nouveaux mots de passe soient utilisés par des utilisateurs légitimes, et non par des tiers qui ont obtenu les données d'identification »[371].

Enfin, ces dispositions techniques devraient inclure les activités en amont (développement applicatif) et en aval (gestion des exemplaires de sauvegarde). À cet égard, il s'agit d'ailleurs « de réaliser une stricte séparation des environnements de développement, test, acceptation/intégration et production et de n'accorder des accès à l'environnement de production qu'aux gestionnaires systèmes dûment autorisés et identifiés »[372].

§ 4. La journalisation

62. Nous avons déjà mis l'accent sur l'importance de l'enjeu de la journalisation ainsi que sur les recommandations de la CPVP et de la CNIL à cet égard[373]. Pour rappel, la journalisation concrétise la propriété d'imputabilité consistant « à enregistrer les informations pertinentes concernant des événements du système au cours de son activité (accès à un système ou à un dossier, modification d'un fichier, transfert de données, envoi ou réception d'un message électronique, réalisation d'une transaction commerciale, etc.), à la manière d'un journal de bord, dans des fichiers appelés *logs* »[374]. Paradoxalement, afin de garantir la protection des données à caractère personnel, l'obligation de sécurité peut donc avoir pour conséquence, selon les besoins, d'imposer un traitement de données à caractère personnel additionnel ou accessoire ayant pour finalité l'imputabilité des actions réalisées sur les traitements initiaux[375].

---

370 CNIL, « La sécurité des données personnelles », *op. cit.*, p. 7.

371 Groupe 29, WP 213, *op. cit.*, p. 9.

372 CPVP, *Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*, *op. cit.*, p. 5.

373 Voy. le § 2 de la section 2 du chapitre 2 de la présente contribution.

374 S. Ghernaouti, *Sécurité informatique et réseaux*, *op. cit.* p. 6.

375 Dans le contexte de la lutte contre l'échange non autorisé de fichiers électroniques musicaux réalisé grâce à des logiciels « peer-to-peer », la C.J.U.E. a estimé que « […] la collecte et l'identification des adresses IP des utilisateurs qui sont à l'origine de l'envoi des contenus illicites sur le réseau [sont] des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs ». Voy. C.J.U.E., 24 novembre, arrêt *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10.

Par conséquent, le Contrôleur européen de la protection des données[376] (ci-après « EDPS ») s'est également penché sur la question et a formulé quelques lignes directrices sur le sujet. Selon celui-ci, il s'agit tout d'abord de tenir compte du principe de minimisation pour définir le contenu des journaux de sécurité et leur durée de conservation en fonction des besoins du débiteur de l'obligation de sécurité[377]. Ensuite, conformément au principe de finalité, les données collectées à des fins de contrôle de la sécurité ne peuvent être utilisées qu'à cet effet[378]. Enfin le Groupe 29 indique que, si les fichiers de journalisation sécurisés sont fiables (c'est-à-dire s'ils ne sont pas compromis), ceux-ci peuvent d'être d'une grande utilité en cas de violation de données[379].

§ 5. Les audits

63. L'article 32, § 1, d), du règlement stipule explicitement que, selon les besoins, doit être mise en place « une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ». Dans le même esprit, l'article 28, § 3, h), prévoit qu'en cas de sous-traitance, le contrat doit obligatoirement « permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ».

La CPVP s'inscrit dans la même logique en recommandant que « l'organisme doit s'assurer que les mesures de sécurité techniques ou organisationnelles sont validées et font l'objet de révisions régulières. Les besoins de maintenance de la sécurité doivent pouvoir être détectés par une surveillance portant sur les traitements, l'évolution des ressources et l'analyse des journaux de traçage. Les systèmes d'information et les risques auxquels ils sont exposés étant en constante évolution, l'organisme s'assurera régulièrement (au moins une fois par an) que les objectifs initialement poursuivis et les mesures de sécurité mises en place consécutivement restent d'actualité afin d'y apporter les éventuels correctifs, si nécessaire »[380].

---

[376] Le Contrôleur européen de la protection des données (en anglais European Data Protection Supervisor - EDPS) est une autorité de contrôle indépendante qui a pour mission première d'assurer que les institutions et organes européens respectent le droit à la vie privée et à la protection des données lorsqu'ils traitent des données à caractère personnel et élaborent de nouvelles politiques.

[377] EDPS, *Lignes directrices sur les données à caractère personnel et les communications électroniques au sein des institutions de l'Union*, décembre 2015, p. 8.

[378] *Ibid.*, p. 9.

[379] Groupe 29, WP 213, *op. cit.*, p. 9.

[380] CPVP, *Mesures de référence applicables à tout traitement de données à caractère personnel*, *op. cit.*, p. 5.

Les organismes s'assureront évidemment de soumettre l'auditeur désigné à une obligation de confidentialité. Par ailleurs, l'article 39, § 1, b), du RGPD met à charge du délégué à la protection des données la mission de contrôler lesdits audits. Un aperçu des principales méthodes d'audit a été publié par l'ENISA en 2013[381].

L'importance des audits est également rappelée par le Groupe 29 selon lequel « un contrôle permanent des vulnérabilités potentielles des technologies utilisées, incluant au moins une analyse régulière des vulnérabilités du site web et une mise à jour des logiciels (y compris des logiciels de sécurité), [peuvent permettre d'éviter une] violation soit de réduire son incidence. Même si les attaques jour zéro exploitant des vulnérabilités de sécurité sont difficiles à éviter, des stratégies adéquates et efficaces permettant d'empêcher de manière proactive l'exploitation des vulnérabilités de sécurité, notamment un examen du code, peuvent réduire la marge de risque à un niveau acceptable. En outre, une bonne politique de gestion des incidents de sécurité peut également réduire les conséquences d'une violation en limitant l'ampleur et la durée de ses effets négatifs »[382].

§ 6. La gestion des incidents

64. Pour rappel, l'article 32, § 1, c), du RGPD impose aux débiteurs de l'obligation de sécurité de mettre en œuvre, selon les besoins, « des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ». De telles mesures ne peuvent se concevoir sans plan de gestion des incidents de sécurité.

Ainsi, selon la CPVP, « en cas d'incidents mettant en péril la confidentialité et l'intégrité des données à caractère personnel, la rapidité d'intervention est primordiale pour réduire les conséquences d'une telle situation. Pour ce faire, l'organisme doit avoir prévu les procédures spécifiant la marche à suivre en cas de détection d'incident de sécurité relatifs aux données à caractère personnel ainsi que les personnes responsables pour gérer l'incident et restaurer une situation saine. En outre, les conditions de l'incident doivent être analysées afin d'en déduire les mesures préventives ou correctrices destinées à éviter la reproduction de ce genre d'incident ou de permettre un retour plus rapide à une situation normale »[383]. De plus, selon

[381] ENISA, *Auditing Security Measures - An Overview of schemes for auditing security measures*, septembre 2013.

[382] Groupe 29, WP 213, *op. cit.*, p. 8.

[383] CPVP, *Mesures de référence applicables à tout traitement de données à caractère personnel*, *op. cit.*, p. 5.

l'APD nationale belge, « les organismes, contraints d'assurer la continuité de leurs services, doivent prévoir les plans de recouvrement et de continuité permettant de couvrir les incidents de sécurité pouvant provoquer des interruptions de service dépassant les délais acceptables et veiller particulièrement à ce que la confidentialité et l'intégrité des données personnelles soient toujours assurées lors de l'exécution de ces divers plans »[384].

La mise en place d'un plan de gestion adéquat est capitale puisque le RGPD considère qu'il « convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs […] »[385].

384 *Ibid.*

385 Considérant n° 87 du RGPD.

CHAPITRE 9. La notification et la communication des violations de données

SECTION 1. – Objet

65. Le concept de « violation de données à caractère personnel » est défini à l'article 4, 12) du RGPD comme étant « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ». Ainsi que nous l'avons déjà mentionné, le Groupe 29 considère que ce concept couvre tant les violations d'intégrité, de confidentialité que celles de disponibilité des données, mêmes si ces dernières sont seulement temporaires[386]. Evidemment, ces différents types de violations de données peuvent avoir lieu séparément ou de manière cumulative[387].

---

[386] Voy. le § 2 de la section 1 du chapitre 2 de la présente contribution.
[387] Groupe 29, WP 250, *op. cit.,* p. 8.

L'article 33, § 1, du RGPD prévoit que le responsable du traitement est tenu de notifier de telles violations de données à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Dans le cas où la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est doit être accompagnée des motifs du retard. Toutefois, cette notification à l'APD n'est pas requise lorsque la violation en question *n'est pas susceptible d'engendrer un risque* pour les droits et libertés des personnes physiques. De plus, lorsqu'une violation de données à caractère personnel est *susceptible d'engendrer un risque élevé* pour les droits et libertés d'une personne physique, le responsable du traitement doit communiquer ladite violation de données à caractère personnel à la personne concernée dans les meilleurs délais[388].

SECTION 2. – Prise de connaissance et délais

§ 1. Le délai de notification

66. En cas de violation de données, l'article 33, § 1, du RGPD impose au responsable du traitement notifier celle-ci à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures[389] au plus tard « après en avoir pris connaissance »[390].

Quant au sous-traitant, le second paragraphe dudit article précise qu'il doit notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais « après en avoir pris connaissance ». Autant dire qu'en cas de sous-traitance, une clause contractuelle précisant un délai plus précis de notification au responsable du traitement est fortement recommandée au risque pour ce dernier de ne pouvoir se conformer au délai « maximum » de 72 heures[391]. De même, « *a processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made*

[388] Art. 34, § 1, du RGPD.

[389] Pour ce qui concerne les règles européennes en matière de calcul des délais, voy. le règlement (CEE, Euratom) 1182/71 du Conseil du 3 juin 1971portant détermination des règles applicables aux délais, aux dates et aux termes.

[390] Art. 33, § 1, du RGPD.

[391] Selon le Groupe 29, « *the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours* ». Groupe 29, WP 250, *op. cit.*, p. 14.

in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller »[392].

§ 2. Le point de départ des délais de notification

67. Le Groupe 29 considère que le moment de prise de connaissance d'une violation de données est celui où il existe un « degré raisonnable de certitude » qu'un incident a eu lieu et que les données sont compromises[393]. Néanmoins, ainsi que nous l'avons déjà mentionné, le RGPD impose un plan de gestion des incidents adéquat « pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée »[394]. Cela étant dit, le moment concret de prise de connaissance dépendra évidemment des circonstances : « *in some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised* »[395]. Le Groupe 29 donne pour exemples :

- le cas d'une clé USB perdue sur laquelle sont stockées des données non chiffrées. Dans cette hypothèse, c'est évidemment le moment de la perte de la clé qui doit être pris en compte ;
- les cas dans lesquels un tiers informe un débiteur de l'obligation de sécurité qu'il a accidentellement ou volontairement obtenu des données et lui en fournit la preuve. Dans ces hypothèses, c'est le moment où la preuve est fournie qui doit être pris en considération ;
- une intrusion potentielle est détectée dans un réseau et le gestionnaire vérifie si des données ont été compromises. Dans ce cas, la prise de connaissance a lieu au moment où l'intrusion est confirmée et qu'elle consiste en une « violation de données ».

Selon le Groupe, dans certaines hypothèses, le moment où « degré raisonnable de certitude » qu'un incident a eu lieu entraînera une courte période d'enquête pour déterminer s'il y'a eu ou non « violation de données » au sens de l'article 4, 12), du RGPD : « *during this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place ; a more detailed investigation can then follow* »[396].

---

392 *Ibid.*
393 Groupe 29, WP 250, *op. cit.*, p. 11.
394 Considérant n° 87 du RGPD.
395 Groupe 29, WP 250, *op. cit.*, p. 11.
396 *Ibid.*

Enfin, en cas de sous-traitance, le Groupe 29 affirme que « *Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller ; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes ; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify* »[397].

SECTION 3. – Les critères de gravité d'une violation de données

68. Afin de déterminer si le responsable du traitement doit se conformer à l'exigence de notification à l'autorité de contrôle et/ou à celle de la communication aux personnes concernées, celui-ci doit respectivement procéder, d'une part, à une évaluation de l'existence de la susceptibilité d'un risque pour les personnes concernées, et, d'autre part de la gravité que ce risque pourrait engendrer pour celles-ci. En effet, la communication aux personnes concernées n'est requise que lorsque la violation de données est *susceptible d'engendrer un risque élevé pour celles-ci*. Le considérant n° 85 énumère des exemples de risques pour les droits et libertés des personnes physiques en cas de violation de données.

Dans ce contexte, il s'agit à l'évidence de tenir compte des conséquences résultant de la matérialisation effective du risque suite à la violation de données. À cet égard, le Groupe 29 estime que « *assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA. The DPIA considers both the risks of the data*

[397] Groupe 29, WP 250, *op. cit.*, p. 13.

processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue ; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals »[398].

Par conséquent, afin d'évaluer le risque pour les personnes physiques résultant d'une violation de données, le responsable du traitement doit prendre en considération les circonstances particulières de ladite violation, en ce compris la gravité et la probabilité de l'impact potentiel pouvant concrètement en découler. Dans cet exercice, le Groupe 29 recommande aux responsables du traitement de tenir compte des facteurs suivants :

- le type de violation[399] ;
- la nature[400], la sensibilité[401] et le volume des données[402] ;

[398] Groupe 29, WP 250, *op. cit., p.* 23.

[399] Selon le Groupe 29, « *the type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost and are no longer available* ». Groupe 29, WP 250, *op. cit.*, p. 24.

[400] Selon le Groupe 29, « *Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child […]. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals* ». Groupe 29, WP 250, *op. cit.*, p. 24.

[401] Selon le Groupe 29, « *Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data* ». Voy. WP 250, *op. cit.*, p. 24.

[402] Selon le Groupe 29, « *Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals* ». Groupe 29, WP 250, *op. cit.*, p. 24.

- la facilité d'identification des personnes concernées[403]. À cet égard le Groupe insiste particulièrement sur l'importance du chiffrement et/ou de la pseudonymisation[404] ;
- la gravité des conséquences pour les personnes concernées[405] ;
- les caractéristiques particulières des personnes concernées[406] ;
- les caractéristiques particulières du responsable du traitement[407] ;
- le nombre de personnes affectées par la violation de données[408] ;

[403] Selon le Groupe 29, « *An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches* ». Groupe 29, WP 250, *op. cit.*, pp. 24 et 25.

[404] Selon le Groupe 29, « *personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible* ». Groupe 29, WP 250, *op. cit.*, p. 25.

[405] Selon le Groupe 29, « *Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm […] Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term* ». Groupe 29. WP 250, *op. cit.*, p. 25.

[406] Selon le Groupe 29, « *A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them* ». Groupe 29, WP 250, *op. cit.*, p. 25.

[407] Selon le Groupe 29, « *The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper* ». Groupe 29, WP 250, *op. cit.*, pp. 25 et 26.

[408] Selon le Groupe 29, « *A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected* ». Groupe 29, WP 250, *op. cit.*, p. 26.

Enfin, le Groupe 29 rappelle que l'ENISA a publié des recommandations pour évaluer la gravité d'une violation de données[409] dont les responsables du traitement et les sous-traitants peuvent s'inspirer afin de rédiger leurs plans de gestion des incidents de sécurité[410].

SECTION 4. – Les violations de données ne devant pas être notifiées

69. Une violation de données doit être notifiée à l'autorité de contrôle que lorsqu'elle est *susceptible d'engendrer un risque* pour les droits et libertés des personnes physiques. Ainsi que le mentionne le Groupe 29, « *this is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority* »[411].

Cette exception à l'obligation de notification est illustrée par le Groupe 29 à l'aide de deux exemples. Dans le premier cas, une clé USB contenant des informations chiffrées et ayant fait l'objet d'un back-up est volée. Dans cette hypothèse, selon le Groupe, « *as long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required* »[412]. Dans le second cas d'espèce, un call-centre fait l'objet d'une coupure de courant entraînant une indisponibilité temporaire des données pendant quelques minutes. Dans cette éventualité, le Groupe considère que « *this is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller* »[413].

[409] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, décembre 2013. Soulignons que ces recommandations ont été écrites en collaboration avec des experts issus des APD héllénique et allemande.

[410] Groupe 29, WP 250, *op. cit.*, p. 26.

[411] *Ibid.*, p. 18.

[412] *Ibid.*, p. 31.

[413] *Ibid.*

SECTION 5. – Les violations de données ne devant pas être communiquées

70. L'article 34, § 3, du RGPD prévoit que la communication aux personnes concernées n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

- le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;
- elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Conformément au principe d'*accountability*, les responsables des traitements doivent être en mesure de démontrer qu'une ou plusieurs des conditions susmentionnées sont rencontrées. Ceux-ci doivent également garder à l'esprit que même si une communication n'est pas initialement requise, elle peut le devenir avec l'écoulement du temps si la susceptibilité d'un risque élevé apparaît. En outre, l'article 34, § 4, du règlement prévoit que « si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie ».

Dans la décision de communiquer ou non une violation de données aux personnes concernées, il s'agit d'être extrêmement attentif aux multiples potentielles conséquences concrètes que ladite violation peut engendrer. Par exemple, dans son avis de 2014, le Groupe 29 avait considéré qu'une « violation de la confidentialité de données à caractère personnel qui ont été cryptées à l'aide d'un algorithme de pointe constitue tout de même une violation de données à caractère personnel, et celle-ci doit être notifiée à l'autorité. Néanmoins, si la confidentialité de la clé de cryptage est intacte, les données sont en principe *incompréhensibles* à toute personne qui n'est pas autorisée à y avoir accès, et la violation n'est donc

pas susceptible de porter atteinte à la personne concernée et ne nécessite dès lors pas de lui être communiquée »[414]. Néanmoins, même en cas de chiffrement, une perte ou une altération de données peut être susceptible d'engendrer des conséquences négatives pour les personnes concernées, par exemple dans le cas où aucun backup n'a été prévu. Par conséquent, dans son avis de 2017, le Groupe 29 estime que, dans le cas d'espèce susmentionné, non seulement une notification à l'APD est requise mais également une communication aux personnes concernées[415].

Enfin, il est intéressant de relever le raisonnement du Groupe 29 en cas d'indisponibilité temporaire de données chiffrées faisant l'objet d'un backup : « *where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident"* »[416].

SECTION 6. – Contenu de la notification à l'autorité de contrôle

71. La notification à l'autorité de contrôle doit contenir, à tout le moins[417] :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la communication, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

414 Groupe 29, WP 213, *op. cit.*, p. 3.
415 Groupe 29, WP 250, *op. cit.*, p. 18.
416 *Ibid.*, p. 19.
417 Art. 33, § 3, du RGPD.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu[418]. Selon le Groupe 29, « *this means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority* »[419].

SECTION 7. – Contenu et modalités de la communication aux personnes concernées

§ 1. Contenu de la communication

72. Lorsque la communication aux personnes concernées est requise, celle-ci doit contenir décrire « en des termes clairs et simples »[420] au moins les informations suivantes :

- la nature de la violation de données à caractère personnel ;
- la communication, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;

418 Art. 33, § 4, du RGPD.
419 Groupe 29, WP 250, *op. cit.*, p. 15.
420 Art. 34, § 2, du RGPD.

- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

L'objectif principal de la communication est de permettre aux personnes concernées de « prendre les précautions qui s'imposent »[421]. Il s'agit donc de « formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels »[422]. Par exemple, dès lors que des mots de passe sont compromis, « le responsable du traitement devrait obliger les personnes concernées à créer un nouveau mot de passe, en mode sécurisé, afin de garantir que tous les nouveaux mots de passe soient utilisés par des utilisateurs légitimes, et non par des tiers qui ont obtenu les données d'identification. Dans la pratique, cela peut correspondre à la procédure sécurisée de renouvellement d'un mot de passe perdu et des informations justifiant le renouvellement du mot de passe devraient être incluses. Dans la notification adressée à l'utilisateur, il convient également de recommander à ce dernier de ne pas réutiliser l'ancien mot de passe ou un mot de passe similaire et de changer les mots de passe compromis pour tous les comptes où le même mot de passe était utilisé »[423].

§ 2. Modalités de la communication

73. Lorsque la communication aux personnes concernées est requise celle-ci doit être réalisée directement envers les personnes concernées sauf si celle-ci exigerait des efforts disproportionnés[424]. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace[425].

Afin d'être transparente, la communication doit être envoyée séparément d'autres informations telles que des updates ou des newsletters[426]. Selon le Groupe 29, « *examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an*

421 Considérant n° 86 du RGPD.
422 *Ibid.*
423 Groupe 29, WP 213, *op. cit.*, p. 9.
424 Art. 34, § 3, c), du RGPD.
425 *Ibid.*
426 Groupe 29, WP 250, *op. cit.*, p. 21.

individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel »[427].

En ce qui concerne l'élément temporel, la communication aux personnes concernées doit, en principe, être réalisée « dans les meilleurs délais »[428], c'est-à-dire « aussi rapidement qu'il est raisonnablement possible »[429]. Néanmoins, il s'agit d'agir « en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires peut justifier un délai plus long pour la communication »[430]. Dans le même sens, le considérant n° 88 du RGPD rappelle qu'il faut tenir compte « de l'intérêt légitime des autorités répressives lorsqu'une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation des données à caractère personnel ».

SECTION 8. – Documentation

74. L'article 33, § 5, du RGPD impose au responsable du traitement de documenter toute violation de données à caractère personnel « en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article ». Cette obligation documentaire est liée à l'obligation d'*accountability* et peut être requise les autorités de contrôle. Il est donc recommandable d'inclure cette documentation dans le Registre[431].

[427] *Ibid.*
[428] Art. 34, § 1, du RGPD.
[429] Considérant n° 86 du RGPD.
[430] *Ibid.*
[431] Pour une description du contenu de cette documentation, lire Groupe 29, WP 250, p. 26.

Conclusion

75. Ainsi que nous l'avons déjà mentionné dans notre introduction, le renforcement de l'obligation de sécurité des traitements de données à caractère personnel dans le cadre du RGPD s'inscrit dans un contexte plus large dans lequel la sécurité des données et des systèmes informatiques est devenu un enjeu majeur pour le législateur européen. En témoignent différentes initiatives telles que la directive NIS, déjà citée, mais également le règlement eIDAS[432] ou encore la directive PSD2[433] qui dépassent le cadre de la présente contribution[434]. Selon le champ d'application de ces instruments[435], les débiteurs de l'obligation de sécurité de traitements de données à caractère personnel devront toutefois en tenir compte, tant en ce qui concerne les mesures techniques et organisationnelles à mettre en œuvre qu'en termes de notification en cas de violation de sécurité[436]. À titre d'exemples, le Groupe 29 cite « *a cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach* »[437].

---

[432] Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. À ce sujet, lire D. Gobert., « L'identification électronique et les services de confiance dans le règlement eIDAS », *J.D.E.*, 2016/7, n° 231, pp. 250-258 ; H. Jacquemin, « Principes applicables à tous les services de confiance et au document électronique », in *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 101-137 ; J.-B. Hubin, « Le cachet électronique des personnes morales », in *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, 2016, pp. 175-202.

[433] Directive 2015/2366/UE du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) 1093/2010, et abrogeant la directive 2007/64/CE (Texte présentant de l'intérêt pour l'EEE). À ce sujet, lire D. Philippe, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », in *Actualités en droit commercial et bancaire*, Bruxelles, Larcier, 2017, pp. 455-477.

[434] Sans oublier le « règlement e-Privacy » en cours de négociations. Voy. Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE, 2017/0003 (COD).

[435] Nous ne prétendons à aucune exhaustivité dans l'énumération des régimes légaux potentiellement applicables selon le contexte.

[436] Groupe 29, WP 250, *op. cit.*, pp. 28 et 29.

[437] *Ibid.*

Ayant rappelé cette tendance, l'objectif de notre texte est avant tout de mettre l'accent sur l'avènement d'un « nouveau » principe de base étroitement lié à l'exigence d'*accountability*. En attestent le fait que tous les responsables de traitements et sous-traitants doivent tenir un Registre dès lors que leurs traitements ne sont pas occasionnels[438] et qu'une évaluation des risques inhérents doit être documentée qu'il y'ait ou non obligation de procéder (ou d'aider à la réalisation) d'une AIPD ; laquelle doit, du reste, être matérialisée dans de nombreux cas.

Enfin, même si l'objet du principe de sécurité aurait mérité davantage de précisions explicites en ce qui concerne l'impératif de disponibilité des données en sus des contraintes d'intégrité et de confidentialité, nous constatons une convergence d'opinions entre le Groupe 29 et l'ENISA en la matière, de sorte que cette troisième caractéristique classique de sécurité reçoive toute l'attention qu'elle mérite. Dans la même ligne, l'absence de mentions expresses relatives aux fonctions d'imputabilité, d'authenticité et de non-répudiation des données dans le texte du règlement est compensée par la jurisprudence européenne et par les recommandations des autorités de contrôle nationales qui préconisent fortement la mise en place de politiques de gestion des accès logiques et de journalisation. Ces dernières confortent à nouveau la *ratio legis* du RGPD selon laquelle sécurité des données et *accountability* vont de pair : une obligation de moyens n'a de réelle puissance que lorsqu'elle est accompagnée de mesures permettant de vérifier si ses débiteurs ont été suffisamment prudents et diligents dans sa mise en œuvre.

[438] À cet égard, lire Groupe 29, Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, 19 avril 2018.